# EXHIBIT C
# Part 1 of 3

VERITEXT
LEGAL SOLUTIONS

Deposition of:

**J. Alex Halderman , Ph.D.**

*February 25, 2020*

In the Matter of:

**Fair Fight Action, Inc., Et Al. Vs. Raffensperger, Brad, Et Al.**

Veritext Legal Solutions
800.808.4958 | calendar-atl@veritext.com | 770.343.9696

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FAIR FIGHT ACTION, et al.,
Plaintiffs,
-vs- Case No. 1:18-cv-05391-SCJ
BRAD RAFFENSPERGER, in his official capacity as Secretary of State of the State of Georgia, et al.,
Defendants.
_____/

THE DEPOSITION OF J. ALEX HALDERMAN, Ph.D.
Taken at 31500 Wick Road
Romulus, Michigan
Commencing at 9:27 a.m.
Tuesday, February 25, 2020
Before Trisha Cameron, RDR, RMR, CRR, RPR, CSR

APPEARANCES:

MR. ANDREW D. HERMAN
Miller & Chevalier
900 16th Street NW
Washington, D.C. 20006
(202) 626-5869
aherman@milchev.com

Appearing on behalf of the plaintiffs.

MR. BRYAN P. TYSON
Taylor English Duma, LLP
1600 Parkwood Circle, Suite 200
Atlanta, Georgia 30339
(678) 336-7249
btyson@taylorenglish.com

Appearing on behalf of the defendants.

INDEX TO EXAMINATIONS

EXHIBITS

(Exhibits attached.)

Romulus, Michigan
Tuesday, February 25, 2020
About 9:27 a.m.

* * *

J. ALEX HALDERMAN, Ph.D.,
having been first duly sworn,
was examined and testified as follows:

* * *

MR. TYSON: This will be the deposition of Dr. Alex Halderman taken by Defendant Secretary of State Brad Raffensperger for the purpose of discovery and all purposes allowed under the Federal Rules of Civil Procedure. And we'll reserve all objections except form and privilege and responsiveness until trial or first use, if that's acceptable.

MR. HERMAN: That's acceptable.

EXAMINATION

BY MR. TYSON:

Q. All right. Well, good morning, Dr. Halderman.

A. Good morning.

Q. Brian Tyson. We met before. It's good to see you again.

A. Good to see you again too.

Q. So I want to go over a couple ground rules just as we get started today. Have you had a chance to have your deposition taken before?
A. I have.
Q. Okay. And so you're going to be familiar with this. For our court reporter's sake, it's best that we don't talk over each other. In conversations, sometimes that's easy to do. Sometimes you will know where I'm going with a question before I get to the question mark. It's best for everybody if you can wait until I get to the question mark, then answer.

It's best also for a yes and no, instead of uh-huh and huh-uh, just because that makes for a clearer better transcript.

And we can take breaks whenever you want to along the way. My only request is that you would answer the last question I asked prior to taking a break.

And there have been times, and it happens in every deposition, where we get to the question mark of a sentence, I don't know what I'm asking, you don't know what I'm asking, no one is -- it's totally confusing. Let me know if that happens, and I'll rephrase the question. So will that work for you?
A. Yes, I understand.

Q. Perfect. All right. So what I want to do is first talk through some pieces of kind of how you got ready for today. Then we'll move into your background and experience and then get to the report. That's kind of the general flow we'll be working with for the day.

So what did you do to get ready for your deposition today?

A. So for the deposition today, I reviewed -- I reviewed material that was produced by Dominion to the plaintiffs that the plaintiffs provided to me that was about -- that was several thousand pages of documentation. And I'm also familiar with the contours of Georgia's system more generally from work that I've done in the past.

Q. So in terms of documents you reviewed, documents from Dominion, did you review any other documents to get ready for today?

A. Other documents beyond what I'm generally familiar with. Let me see. I went back and looked at documentation prepared in testing the Dominion equipment in California, as well as the Poll Pads in California. I reviewed certifications from Pennsylvania regarding the Poll Pads and the Dominion equipment, I think documentation from Texas, and a

number of other resources that are cited in my report.

Q. Did you review any documents that are not cited in your report to get ready for your deposition today?

A. I don't believe so. Not specifically for the deposition today. Perhaps the order from the Curling case. I reviewed that.

Q. And that would be the 2019 order?

A. Judge Totenberg's order in 2019. That's correct.

Q. Got it. And did you talk with anybody about your deposition today?

A. I spoke to -- I spoke to Andrew and to Kurt, the attorneys for the plaintiffs.

Q. Anybody at the university who's not an attorney that you spoke to?

A. No.

Q. Anyone else who's not one of the attorneys that you talked to about your deposition today?

A. No. No.

(Exhibit No. 1 marked.)

BY MR. TYSON:

Q. Okay. I'm going to hand you what we've marked as Exhibit 1, the Notice of deposition. I'm assuming you've seen that document before.

A. Yes, I have.

Q. Okay. That's just your notice. Then what I'm going to do is go ahead and mark your reports. That way we can refer to it as we're going through the biographical details. That will be easy enough on that. So I'll hand you what we've marked as Exhibit 2.

(Exhibit No. 2 marked.)

BY MR. TYSON:

Q. I'll ask if that's the report that you filed in this case.

A. Yes.

MR. HERMAN: Can I just note for one second, this is the unsigned version.

MR. TYSON: Right. I'm going to hand him --

(Exhibit No. 3 marked.)

BY MR. TYSON:

Q. So I'll hand you, make it complete, what I've marked as Exhibit 3.

A. Yes.

Q. Is that the signature page for the report that is Exhibit 2?

A. Yes.

Q. Okay. Wonderful.

MR. HERMAN: I underestimated you.

I'm sorry.

MR. TYSON: Totally fine.

BY MR. TYSON:

Q. All right. So, Dr. Halderman, in paragraph 13 of your report, you indicate that you're being compensated at a rate of $750 an hour for your work on this case, correct?

A. That's correct.

Q. And is that -- you indicate that's your customary rate. Do you provide discounts for your expert services in other cases, or is that what you charge for all services?

A. I generally don't provide discounts.

Q. And when you say you generally don't, are there specific situations where you have?

A. There's -- I can think of one other situation I have where work involved -- work involved a large amount of rote technical work that I could do on an arbitrary timeline, in which case I have.

Q. And is the rate of $750 an hour generally what you charge when you're working on a technical review for a state or other sorts of work like that?

A. Well, it depends on the circumstances. The work that I would do for a state might be anywhere from pro bono to the $750 rate.

Q. Do you know approximately how much time you spent preparing your report?
A. I don't recall exactly how much time.
Q. And have you sent a bill in this case?
A. I haven't yet.
Q. Okay. And you plan to?
A. I plan to.
Q. Okay. And you don't have a current estimate of what that amount will be?
A. No, I haven't prepared the bill yet.
Q. All right. So let's talk a little bit about how you got involved in this lawsuit. Did someone contact you about providing a report in this litigation, or how did you get started being an expert in this case?
A. I was contacted by Plaintiffs' Attorneys I suppose approximately a year ago. I'd have to go back and check.
Q. And when you were contacted, did anyone give you direction about what you were supposed to examine beyond what you've described in your report?
A. No, I don't believe so.
Q. Did Plaintiffs' Counsel provide you with any data or documents for purposes of this report?
A. Yes. They provided me with material that they -- that was the result of a subpoena to Dominion.

Q. And I should have asked. Beyond the Dominion subpoena documents, did Plaintiffs' Counsel provide you any other data or documents that you relied on?
A. Nothing beyond what's in the docket.
Q. And did Plaintiffs' Counsel ask you to make any assumptions about facts in this case for your report?
A. No, they didn't.
Q. Have you read the amended complaint in this case?
A. Yes, I have.
Q. Have you read any of the depositions that were taken in this case?
A. I don't believe so.
Q. You indicated some docket information. Have you read any of the briefs that were filed in this case?
A. I have -- I've skimmed through the docket, and I've read some of the materials. I'm not sure I've read any of the briefs in full.
Q. I'm not asking for your legal opinion here. But in your own words, do you have a description of what you believe this case is about?
A. So this case is broadly about whether election practices in the state of Georgia have violated the rights of Georgia voters or had discriminatory effects.
Q. And for your report and your work in this case,

you're not alleging any racial component to any of the problems that you've identified in your report, correct?

A. Well, the problems that I have discussed in my report certainly could have a racial effect, especially if an attacker seeking to so discord or alter the outcome of an election targeted specific candidates or racial groups for that effect.

Q. For purposes of this report, though, you have not examined any racial impacts that -- you can speculate about there might be one. But for purposes of your report here, you're not alleging there are any racial impacts, correct?

A. I haven't gone back to examine racial data.

Q. Okay.

A. But certainly one of the risks, the problems that I identify in this report could have is racially disparate impacts.

Q. And the opinions that you've authored in this report in Exhibit 2 do not address the potential racial impact, correct? You're not analyzing -- let me start over again.

The opinions you're expressing in Exhibit 2 are not an analysis of any racial effect of particular methods of attack. Is that a fair

statement?
A. Well, they raise the possibility that -- and describe methods by which an attack could occur that I think it's clear could have a racial impact. Do I analyze exactly what that impact would be? I think that depends on what the attacker is hoping to achieve.
Q. Maybe I can put a finer point on this. In the opinions you're expressing in your report, you're not alleging that Georgia has selected particular voting machines or voting practices to have a racially disparate impact, are you?
A. I'm not alleging intention.
Q. And you're not expressing any opinion about intention; is that correct?
A. No, I don't go to intention.
Q. As part of your work on your report, have you spoken to anyone in Georgia to obtain any information that you later used in your report beyond Plaintiffs' Counsel?
A. I have had past conversations with people in Georgia that have informed my -- that have informed my overall knowledge about Georgia election systems.
Q. And who would those individuals be?
A. I've spoken to Dr. Richard DeMillo at Georgia Tech and Dr. Wenke Lee at Georgia Tech. That's just two

individuals. And I have -- those would be probably the two primary people who have informed my -- helped inform my general knowledge about Georgia elections.

Q. Have you spoken to any county election officials in Georgia?

A. No, I don't believe so.

Q. Have you spoken with anyone in the Secretary of State's office that resulted in information that was included in your report?

A. No. But I'm generally familiar with their testimony and the Curling matter and earlier litigation.

Q. And when you refer to earlier litigation, beyond Curling, what are you referring to there?

A. Boy, all of this litigation has been going on for a while, hasn't it? I think there was -- am I correct there was a state matter that -- before the Curling federal matter in which there was additional testimony?

Q. Does Favirito versus Handel as a state court matter ring a bell? If not, that's fine. I just thought I could help identify it for you. But if not, that's fine.

A. I'm sorry.

Q. No problem. Let's talk a little bit about your kind of journey to here, starting with your undergraduate

work at Princeton. I know that you had your CV attached to your report. So I just want to walk through a few questions on that.

Your thesis for undergraduate work you indicate was titled Investigating Security Failures and Their Causes, An Analytic Approach to Computer Security.

Can you tell me a little bit about how you arrived at that topic? I'm sorry. That was your Ph.D. thesis. I misspoke on that.

A. How I arrived at that topic? Can you -- what do you want to know?

Q. Sure. So you focus obviously on computer security and those types of issues. How is it that you arrived at wanting to study or studying this particular area, cybersecurity?

A. I see. I started working on studying security questions even when I was an undergrad at Princeton. So you'd have to go back even farther. But I suppose what interested me most about security was that it bridged both technical problems that were of significant technical interest and problems involving human beings and their lives, and there was an opportunity in security to -- there was an opportunity in security to bridge both the technical

and the human elements.
Q. And I know from a timing perspective we're looking at kind of post-2000 election. I'm assuming that the rise in electronic voting around the same time period, was that also a factor, seeing the changes in the growth there?
A. I'm not sure that that is what initially attracted me to the security field. I had already been working in the area, but the rise of electronic voting at the time was certainly one of the challenging new research problems that was exciting.
Q. I see you finished up in Princeton in 2009. And then where did you go from there before arriving at the University of Michigan?
A. I came directly to the University of Michigan.
Q. Oh, I see. I'm sorry. I was looking at the top line there. As an assistant professor?
A. That's right.
Q. And so are you currently tenured at the University of Michigan?
A. I am.
Q. And your entire academic career as a professor has been at the University of Michigan, correct?
A. That's correct.
Q. And was there a particular item or issue that led you

from Princeton to Michigan?
A. Not really. Michigan -- Michigan has a very well-ranked computer science department and has one of the best computing systems groups in the country, which is the broader area in which most security research lies.
Q. And so in terms of courses that you are teaching, you list some of those on there. You've taught courses on election, cybersecurity. It's fair to say that your focus really has been on cybersecurity in the election context; is that a fair statement?
A. That has been one of the large focuses of my work. But my work is about computer security and cybersecurity broadly, also work about encryption technology, about securing devices attached to the internet, and so on.
Q. And based on the courses you have in your CV, ethics is also a part of the questions you have to deal with; is that correct?
A. Yes. That's correct.
Q. And so in terms of kind of general principles of ethical implications involved with cybersecurity work, what are some topics that you cover with your students on those areas?
A. Questions like responsible disclosure, that is

informing manufacturers of vulnerabilities in a way that helps get the vulnerabilities fixed. Questions about when is it right or lawful or not to conduct an assessment of a particular system, etcetera.

Q. And when you say when it's right or lawful to conduct an assessment of a particular system, can you elaborate on that for me real quick?

A. Well, there are sometimes when there are some vulnerabilities in systems that are too dangerous to investigate without the cooperation of the people running a system because by virtue of investigating them, you might disrupt the system in a way that causes broader damage. For instance, trying to without permission demonstrate ways that you could hack into a hospital, which might have the effect of causing people to die. That's probably not an ethical exercise in hacking. If there are safer alternatives, it would be preferred to attempt those safer alternatives.

Q. And then do you do any consulting or offer services to companies that want you to investigate potential vulnerabilities that they have?

A. I have a startup company that I founded that is in the business of helping companies understand the vulnerabilities in their internet-facing systems.

Q. And so I'm assuming the business model is a company would retain your services through your corporation -- through your company to help them evaluate that?
A. No. It's not so much about retaining my services. But we produce application software that helps companies understand their exposure.
Q. And what is the name of your company?
A. It's called Censys, C-e-n-s-y-s.
Q. And do you sell the software that helps companies understand their exposure?
A. It's kind of an annual license model.
Q. And then after a company understands its exposure, does Censys offer services to help it mitigate those risks?
A. Yes, essentially.
Q. And is that more on a consulting basis as opposed to the annual license model?
A. No. It's not really a consulting model. We help to point out what the vulnerabilities are and help you understand which ones are important to mitigate.
Q. And I'm assuming in your work with Censys and then your work at the University of Michigan you never encountered a system with zero vulnerabilities. Is that safe to say?

A. Yes. I think that's probably safe to say, that computing systems in general of more than trivial complexity as a rule have vulnerabilities.
Q. And in your work with Censys, are there situations where a company is not able to mitigate all the vulnerabilities you identify?
A. Well, not able is a bit of a tricky statement. So I think it's a question of -- all of the vulnerabilities that we identify are things that can be mitigated.
Q. And then it's up to the company to choose whether or not they want to mitigate those vulnerabilities, right?
A. That's right. Nobody forces anyone to mitigate vulnerabilities in general.
Q. And so ultimately, I guess maybe this is too general of a statement, but there are companies that choose to encounter a level of risk for some reason known to them?
A. Well, that's right. And sometimes -- sometimes that's clearly irresponsible.
Q. Can you tell me about ISRG and what that is.
A. Sure. ISRG, the Internet Security Research Group, is a not-for-profit company that I co-founded.
Q. And what type of work does ISRG do?

A. So ISRG runs some of the critical security infrastructure for the internet. It runs a service called Let's Encrypt, which is a certificate authority. That means that it vouches for the identity of websites. So if you connect to a website that has https, one of the crucial steps that's going on behind the scenes before you make that connection is that some trusted authority has vouched for the identity of the site so that your computer knows it's talking to the real website and not to an attacker. So ISRG and Let's Encrypt are the worlds largest certificate authority. They've issued a billion certificates as of this week for several hundreds of millions of websites.

Q. Have you ever seen a situation where an attacker attempted to appear to be a certificate authority to gain access to a system.

A. Yes.

Q. Is that a fairly typical method of trying to attack or hack a system?

A. To pretend to be a certificate authority? It's one of the attacks that we as a security community spend a lot of time trying to make sure it doesn't happen.

Q. But it is a potential risk --

A. Yes.

Q. -- correct? Are you paid for your services with ISRG?
A. No. I only receive compensation for my travel.
Q. And I'm assuming you are paid for the services Censys provides, correct?
A. Yes, I am.
Q. So you benefit when there is a -- having visibility about exposing vulnerabilities is a benefit to you as advertising for Censys. Is that fair to say?
A. I suppose. It depends on what the context of that vulnerability is.
Q. You indicate in your CV that in 2011 you received the Election Verification Network's John Gideon Memorial Award. Do you recall that?
A. Yes.
Q. And what is the Election Verification Network?
A. The Election Verification Network is a -- is a group of election technology experts and election officials and -- who are -- who work in the topic area of increasing the security of elections.
Q. And I'm assuming you've participated in EVN conferences in the past?
A. I have, yes.
Q. And what does the John Gideon Memorial Award recognize?

A. I think it's scoped as recognizing contributions to election integrity.

(Exhibit No. 4 marked.)

BY MR. TYSON:

Q. Dr. Halderman, I'm going to hand you what we've marked as Exhibit 4. And this is the -- appears to be -- well, it's from the website of EVN for the 2019 conference. And if you could turn over to the third physical page.

A. Page 3?

Q. Yes.

A. All right.

Q. There's a 1:45 p.m. session on usability and voter verification. Are you with me on that?

A. Yes.

Q. And was this one of the panels for EVN on which you appeared?

A. I don't believe I appeared on that panel, no.

Q. Okay.

A. But I'm not listed as a panelist, and I don't recall being on that panel.

Q. At the -- I see your name right there. I see Josh Benaloh from Microsoft, Michelle Bishop, and then J. Alex Halderman.

A. Excuse me. I was looking at the 11:45. You mean the

1:45 panel?

Q. Got it. My apologies.

A. Yes. That panel I did speak on.

Q. And can you tell me a little bit about what usability and voter verification, what topics this panel covered?

A. Yes. So this panel was about -- this panel was in part about ballot marking devices and the issues of usability and accessibility connected to them. It was also in part about what are called end-to-end verifiable voting protocols and accessibility and usability attributes connected to them.

Q. And maybe I can get some definitions of terms. So when you say the usability attributes of a system, what is that referring to?

A. It refers to -- it refers to how humans interact with the technology and whether they're able to use it correctly and securely.

Q. And accessibility as a topic, what does that cover?

A. Potential -- primarily that covers problems that may involve voters or other users who have certain disabilities, such as physical disabilities, and their ability to use the technology.

Q. And when you refer to end-to-end encryption, can you describe that a little bit, please.

A. So end-to-end verifiable voting protocols are a family of technologies that use advanced encryption methods to provide assurance that the election results were correct essentially.
Q. And that's an area that's still being researched, or are there products available today that provide that?
A. There are products available today that provide that. But it certainly is still actively being researched, and there were some significant limitations to the products that provide it today.
Q. Let me hand you next what will be marked as Exhibit 5.

(Exhibit No. 5 marked.)

BY MR. TYSON:
Q. And this is from the EVN website affiliated organizations. Are you aware of affiliated participating organizations within EVN?
A. I'm aware of some organizations that are affiliated or participating, but I'm not sure that I've seen this list before.
Q. Okay. And my main question, I see organizations like the South Carolina Progressive Network, Common Cause, the Brennan Center, the Advancement Project. And I -- my question is just going to be, do you know if there are any conservative lean organizations

affiliated with EVN? If you don't, that's fine.
A. I don't know the politics of each of these organizations. I'm sorry.
Q. Easy enough. So let's talk a little bit about the expertise here. You're an expert in cybersecurity. You focused on elections, as we've talked about.
Do you consider yourself an expert in election administration?
A. In election administration? The subset of election administration that concerns securing elections I do consider myself an expert.
Q. Okay. But not in election administration broadly?
A. Not in all aspects of election administration.
Q. And so one of those areas within election administration where you would not be an expert is on, for example, best practices on chain of custody for paper ballots; is that true?
A. That concerns security. So I do think I have some expertise there.
Q. Okay. Which components of election administration do not involve security that you would not consider yourself an expert in?
A. Well, I suppose not being an expert, I can't identify all of the expert -- the areas that I lack expertise in.

Q. Well, and the reason why I ask is in terms of designing an election system, ultimately every piece of design of an election system has to touch on security in one way or another. Is that fair to say?
A. Probably significant amounts of the design of an election system do. I wouldn't say that every part does.
Q. And we have stories of, I'm sure you've heard, of paper ballots being thrown into rivers, being transported various methods between polling places and central offices. Do you consider yourself an expert on the design of those components of handling paper ballots?
A. Yes, I do have expertise that's in that area.
Q. And do you consider yourself an expert in the design of auditing practices for elections?
A. Yes. Yes, I do.
Q. Let's talk next about your testimony to congress. I'll start with your most recent testimony. You testified to the House Appropriations Subcommittee on Financial Service and General Government in 2019. Do you recall that testimony?
A. Yes, I do.

(Exhibit No. 6 marked.)

BY MR. TYSON:
Q. I'll hand you what we've marked as Exhibit 6. I'll ask if this is your written testimony for that committee.
A. Yes, it appears to be.
Q. And almost a year ago almost to the day, not quite. So --
A. Has it really been only a year?
Q. 2019 was a long year.
MR. HERMAN: Wait until 2020.
BY MR. TYSON:
Q. All right. So in the second paragraph beginning three years ago, you reference hackers penetrating or manipulating efforts and targeting election infrastructure, including voter registration systems in at least 18 states. Was Georgia one of those 18 states?
A. Yes, it was.
Q. Okay. And so it's your testimony that hackers targeted Georgia's voter registration system?
A. So it's my testimony that subsequent to what I -- to my written testimony from a year ago, the Senate Intelligence Committee investigation has concluded that the Russian -- the scope of the Russian attacks was likely all 50 states, which would include

Georgia.
Q. And it's your testimony that that included Russian attacks on Georgia's voter registration system, not just on other components of the election system?
A. I think that it's a fair inference from the findings of the Senate Intelligence Committee that parts of the system that are exposed to the internet like the registration system were among those that the Russians were targeting.
Q. And when you say a system was targeted, you're not necessarily saying it was accessed, correct?
A. Not necessarily.
Q. And not necessarily that it was manipulated in any way, correct?
A. Certainly not that -- you certainly can't conclude from that that it was successfully manipulated. No.
Q. In the next paragraph, the end of that paragraph you say, we were spared such a blow to the foundations of American democracy only because Russia chose not to pull the trigger.
A. That's right.
Q. And so would that be consistent with targeting but not manipulating, that those are two different things?
A. So what we know is also, again, this is from the

bipartisan findings of the Senate Intelligence Committee, is that in one or more states, Russia had the technical ability to manipulate or destroy voter registration data.

Q. But it's not your testimony that Russia had that ability as to Georgia's voter registration system; is that correct?

A. Well, so it's not my testimony that the Senate Intelligence Committee has concluded that Russia had that ability in Georgia. Could Russia have done that in Georgia? I think it's very likely.

Q. Okay. But you don't have any personal knowledge or anything that would indicate to you that Georgia's voter registration system was accessed or could have been accessed by the Russians?

A. Could have been accessed by the Russians? I think based on what I know about the security posture of the Georgia voter registration system and about the capabilities of the Russian attackers, I do think it's likely that they could have accessed it.

Q. Okay. But you don't have any personal knowledge that it was, in fact, accessed?

A. No, I don't.

Q. On the second --

A. When do you think your section will be done just

so -- I think we're getting kind of closer to an hour.

Q. Sure. Maybe five, ten minutes. Do you want to take a break now?

A. All right. We'll take a break after that. Let me stretch.

Q. Sure. We can finish this document, we can do that.

A. Of course.

Q. So on the second physical page, you identify three essential measures to protect and defend our election infrastructure. And the first you indicate is to replace obsolete and vulnerable voting systems, such as paperless systems with optical scanners and paper ballots.

Are you including ballot marking device systems in that as an option that we should look to move to or exclusively hand-marked paper ballots?

A. Ballot marking devices are important in any system that uses paper ballots in order to provide an independent accessible voting option for voters with disabilities. But crucially, the risk of using ballot marking devices becomes very substantial when they're used for all voters, as Georgia does, as opposed to just for voters who request them, for instance, a smaller fraction of voters.

Q. Would you say it's better from a security standpoint for a state to replace a paperless system with a system that involves at least some paper?
A. Depends what they do with that paper. If they don't look at that paper or they're not looking at enough of that paper, then the paper isn't serving the purpose.
Q. And that's true of a hand-marked paper ballot system or a ballot marking device system, correct?
A. If they don't look at it, that's right. It's that the paper isn't serving a purpose.
Q. And which leads us to the second piece there, advocating looking at the paper. And you advocate what's best -- what's known as a risk-limiting audit; is that correct?
A. Yes. I recommend RLAs.
Q. So an RLA, you recommend that whether a state is using hand-marked ballots or ballot marking device ballots, correct?
A. Yes, I do.
Q. On the next page, page 3, you point out that paper ballots, manual audits, and security best practices are endorsed by a lot of folks, including the National Academies of Science, Engineering, and Medicine. I know we had this discussion previously.

But you disagree with the National Academy of Sciences as to ballot marking devices; is that right?

A. No, I wouldn't say that I disagree. The National Academies' report called specifically for further research. And to the question of validation on voter verification of ballot marking devices and ballots that they produce, substantial subsequent research, including research that my own group has conducted, has led to further understanding of the security risks of ballot marking devices.

Q. At this point, the National Academy of Sciences has not changed its recommendation recommending that states use either hand-marked paper ballots or ballot marking devices, correct?

A. I believe they'd have to go through a new consensus report process in order to change what they've written, and that's a process that hasn't happened yet.

Q. So that's a no, they haven't changed their recommendation yet?

A. They have not changed the published report. They haven't released the new recommendation.

Q. Down at the bottom of page 3, you indicate that many states would like to replace vulnerable and obsolete equipment, but they are struggling to figure out how

to pay for it. So you would agree with me that there are a lot of considerations for states in looking at replacing voting equipment, including financial, correct?

A. Yes.

Q. Then on the bottom of page 4, you refer to voter-verifiable paper audit trails, VVPATs.

A. Yes.

Q. And you indicate those are badly inferior to paper ballots. Are they inferior to ballot marking device paper ballots as well?

A. Let me see what I've written here. Excuse me just a minute.

Q. Take your time.

A. So VVPATs are inferior to certain kinds of ballot marking device ballots, but they do share some of the problems of ballot marking device ballots.

Q. I'm assuming that VVPATs and ballot marking device ballots, they are both superior to paperless DREs?

A. When combined with rigorous audits, they're both an improvement. The limitation is -- one of the key limitations has to do with particularly close elections and whether the verifiable paper trail in either case accurately reflects voters' intentions.

Q. Okay. All right. That's all I have for that

exhibit. So we can go ahead and take a break for a few minutes.

A. Okay.

(Recess taken.)

BY MR. TYSON:

Q. Dr. Halderman, next I want us to talk about your testimony to the Senate Intelligence Committee in 2017. How were you invited to attend the US Senate Intelligence Committee, if you recall?

A. How was I invited? One of the -- one of the committee staffers e-mailed me and invited me to testify.

(Exhibit No. 7 marked.)

BY MR. TYSON:

Q. I'm going to hand you what we've marked as Exhibit 7. Is that your statement to the Senate Select Committee on Intelligence?

A. This is my written statement.

Q. If you could turn with me to page 2. You talk about in the second paragraph that optical scanners and DRE voting machines are computers. Then the third sentence you say, fundamentally, they suffer from security weaknesses similar to those of other computer devices.

You'd agree that anything that is a

computer has possible security vulnerabilities?
A. Yes, in general.
Q. And I think, as we talked about earlier, that's true of any computer. There's going to be some vulnerability that a dedicated researcher could find. Fair to say?
A. Yes, that's fair to say. That's why there's some applications in which we shouldn't blindly trust computers to function correctly.
Q. And you mention optical scanners in this group. Is that why you advocate for audits even for hand-marked paper ballots counted by optical scanners?
A. Yes. Essentially that because optical scanners can be hacked so that they count incorrectly, it's important to verify that the election outcome is correct through physical inspection of the records that match the voters' intent.
Q. On the third page, first full paragraph, you mention that vulnerabilities are endemic throughout our election system.

If a jurisdiction was using exclusively DREs and then moved to a hand-marked paper ballot system counted by optical scanners but did not utilize any audits whatsoever, would you consider that more or less secure as an environment?

A. But did not utilize any audits. I would characterize it as a small improvement, although still a significant security risk, such as such a system could withstand, for instance, the total sabotage of the optical scanners and still produce an election result.

Q. But it could not withstand a hacking of the optical scanners that was never discovered because there were no audits, correct?

A. That's correct.

Q. If you could turn with me to page 5. The very top of page 5 and then the first full paragraph on page 5 discuss the Russians being in a position to sabotage equipment causing the failure of voting machines, resulting in long lines, and then putting the Russians in a position to spread an attack and potentially steal votes.

Is there any evidence that the scenarios outlined in those first two paragraphs on page 5 occurred in an election?

A. There is evidence that Russia did attack one or more vendors of election technology and attempt to spread from there to the systems of municipalities. There is -- I think it's a remaining question whether they got any farther than that.

Q. And so is there any evidence that the Russians have sabotaged equipment on election day?
A. So there are failures of equipment on election day that there is I think it's fair to say substantial question whether that failure is the result of an attack or just of other forms of human error.
Q. But sitting here today, you don't have any evidence that equipment failure on election day was caused by a Russian attack, correct?
A. How would we have evidence one way or another? most -- there have been few or no examinations of polling place equipment since 2016 that would reveal one way or another conclusively whether attacks had been successful.
Q. So let me ask again. So sitting here today, you don't have any evidence that any failure of equipment on election day was caused by Russians, correct?
A. No. I cannot say that with high certainty that failures were caused by Russia.
Q. And you're not testifying to the Senate Intelligence Committee or in your report here that -- I should strike that. Let me go to the next one.

And you don't have any evidence sitting here today that the Russians have stolen votes as a result of an attack on voting machines, correct?

A. No, there is no evidence to my knowledge that that did take place. It's -- the problem is that there was nothing technical stopping that from taking place in certain jurisdictions.

Q. But as we discussed in your prior testimony, just because you have the ability to aim the gun doesn't mean you're going to pull the trigger, correct?

A. No, that's right. As I say, Vladimir Putin apparently decided not to pull the trigger, and that's what stopped massive chaos in 2016.

Q. And in the third full paragraph on page 5 you say you don't know how far the Russians got in their effort to penetrate our election infrastructure, nor whether they interfered with equipment on election day. And sitting here today, you still don't know how far they got, correct?

A. Unfortunately, that is correct. There are still large areas of election infrastructure that have not been -- that have not been analyzed since 2016 in a way that would allow us to know. We may never know how far the Russians got.

Q. On page 6 you're reiterating the points of what you recommend for safeguarding elections, and this testimony obviously is in 2017. So in the first bullet when you advocate optical scanners and paper

ballots, at this time in 2017, were you also including ballot marking devices for all voters or only for those with disabilities?

A. I don't say one way or another in this testimony. And I think that at that time, I still would have said the safer thing to do is to limit the use of ballot marking devices to less than all voters.

Q. Have you had a change of your view of ballot marking devices between 2016 and today based on the research you've conducted, or have you always taken the position that ballot marking devices for less than all voters is the best system?

A. I think that my view has gone from one of the conservative positions that ballot marking devices are less safe than hand-marking to one that is the strong research supported conclusion is that ballot marking devices are far less safe. But I think -- I think at the time that this was written back in 2017, I would have acknowledged that we don't yet have enough evidence to conclude strongly one way or the other about ballot marking devices.

Q. In your CV, you also reference five congressional briefings between May 2017 and September 2019. What did those briefings involve?

A. Those briefings involved generally public meetings on

Capital Hill somewhere in which I tried to educate members of congress and their staff about some of the security risks involved in elections.

Q. And were those briefings focused on the vulnerabilities inherent in DREs, or did you discuss other topics related to election security?

A. I discussed other topics too.

Q. And do you recall what those other topics would have been?

A. Well, in general, the threats of -- threats of tampering with other kinds of voting machines, like optical scanners or ballot marking devices. They would have covered risks in other components of the election infrastructure like registration or reporting.

Q. Have you reviewed the Senate Intelligence Committee's report on Russia specifically involving the efforts to interfere with election infrastructure?

A. Yes.

Q. I'm going to hand you what we've marked as Exhibit 8.

(Exhibit No. 8 marked.)

BY MR. TYSON:

Q. And I'll ask is this a report from the Senate Intelligence Committee that you have reviewed previously?

A. Yes, I have reviewed this.
Q. I just want to ask a few questions, kind of walk through this. If you could turn first to page 3. Under the heading that indicates findings, the first paragraph obviously redacted on a number of points. Then the unredacted last sentence, the committee has seen no evidence that any votes were changed or that any voting machines were manipulated.

You'd agree that the committee had access to more information than you had access to in terms of Russia's activities, right?
A. I would. Although, I would note that this is carefully phrased, that they've seen no evidence. So it's, again, acknowledging the limits of the capabilities of the intelligence community to acquire such evidence, especially from systems that just don't generate that kind of evidence.
Q. And it's not your testimony that votes were changed in any election, right?
A. No, it's not.
Q. And it's not your testimony that any voting machine used in an election was manipulated, correct?
A. No, it's not my testimony that any voting machine was manipulated. It's my testimony that the possibility was there and that in significant cases if it had

occurred, we might not know it.
Q. If you could turn next to page 11. Are you familiar with Dr. Liles who testified to the committee?
A. I'm sorry. Where are you referring to?
Q. Page 11.
MR. HERMAN: At the top.
THE WITNESS: Oh, I see. I see.
BY MR. TYSON:
Q. First bullet at the top. Do you know who Dr. Liles is?
A. I don't recall who Dr. Liles is actually.
Q. Okay. Let me ask about the quote that's there. Scanning for vulnerabilities, quoted in the report, is analogous to someone walking down the street and looking to see if you are home. A small number of systems were unsuccessfully exploited as though someone had rattled the doorknob but wasn't able to get in. However, a small number of the networks were successfully exploited. They made it through the door.
Do you agree with that quote that's there in terms of the activities that you're aware of in the 2016 election?
A. With regard to the voter registration system activities, I do agree with that characterization.

Q. Do you agree with -- would you use this description for any other systems beyond the voter registration systems?
A. I'm not sure I would use this description for other systems beyond voter registration.
Q. And why is that?
A. Because the pattern of activities that involved attempts to infiltrate vendor systems and then spread to municipalities, those don't have this form of just rattling the door. Those were -- those were a different shape of attack.
Q. Okay. Let's go next to the next page, page 12. Right before the extensive series of redactions, there's a statement that intelligence developed later in 2018 bolstered Mr. Daniel's assessment that all 50 states were targeted.

Is that consistent with your understanding of Russia's activities in the 2016 election?
A. Yes, it is.
Q. And as we've discussed, targeting is not necessarily the same as manipulating or accessing.
A. That's right. It's probably step one.
Q. Let's go now to towards the very end, page 59.
A. Oh, 59.
Q. Yeah. Way towards the back. So the page immediately

prior, just for context, the recommendations of the committee to secure the vote itself. The first bullet there recommends the purchase of more secure voting machines and recommends that any machine going forward should have a voter-verified paper trail and remove or render inert any wireless networking capability. Do you agree with that recommendation?

A. You're talking about the first bullet here?

Q. Yes.

A. On page 59. I'm just making sure I'm looking at the right -- I would go farther than that recommendation, but I think that -- but I don't disagree with that as it stands.

Q. And as I understand your testimony so far, you would say that this recommendation is not true of Georgia's new voting system; is that correct? Or is it true of Georgia's new voting system?

A. So I think this does apply to Georgia's new voting system. But as I said, I think just this recommendation by itself is not enough to render the voting system secure, and I would certainly go farther.

Q. So to make sure I have that right, you believe Georgia's system complies with the recommendation of this first bullet of the committee's recommendations,

but you would go further than the committee, correct?
A. Yes. Based on the science that's happened since 2017 or since -- since the committee received its testimony that's the basis of this. Yes.
Q. And the second bullet on that page indicates that states should require that machines purchased from this point forward are either EAC certified or comply with the VVSG standards. That's true of Georgia's new system as well, correct?
A. Yes. I believe that is true of Georgia's system.
Q. The third bullet recommends that --
A. Although, actually, pardon me, I'm not sure about the remainder of that bullet, whether Georgia's contracting satisfies that. So if you're talking about the whole recommendation, my answer is I don't know.
Q. Got it. So as to the first sentence, yes. As to the second sentence, you don't have enough information to know.
A. Not at this -- at this time.
Q. The third bullet there indicates an effort to secure the chain of custody for paper ballots, and there's a recommendation related to time stamping when ballots are scanned. Do you see that recommendation?
A. Yes.

Q. And do you know if Georgia's new system includes any safeguards against the insertion of fraudulent paper ballots?
A. Any safeguards against the insertion of fraudulent paper ballots? I think there are some safeguards.
Q. The fourth bullet recommends audits, as we've discussed a little bit already. And there's an indication that as of August 2018, five states conducted no post-election audit and fourteen do not do a complete post-election audit. Do you see that statement?
A. Yes, I do.
Q. And in terms of the adoption of risk limiting audits on a statewide level, do you know how many states currently do a statewide risk-limiting audit?
A. It's a small number. It depends how you want to define it exactly. But perhaps two or three require one at this point.
Q. And when you say it depends on how you want to define it, are there different definitions of risk limiting audits?
A. There are -- there are several complexities to RLA legislation. The question is also about when the audit is required to be performed.
Q. So some of the factors would be whether the audit is

pre-certification or post-certification, correct?
A. Yes.
Q. And some of the factors would be what level of risk limit is set for the audit?
A. Yes.
Q. And so those variabilities affect how robust the audit is. Is that a fair way to characterize that?
A. Those are among the factors that affect whether it's likely to discover an attack, if one occurs.
Q. And are you aware of Georgia's statutory requirements related to risk limiting audits?
A. Yes, I am.
Q. And what do you -- I'm sorry. You're aware that that requires a pilot risk-limiting audit, correct?
A. I'm aware that it does require a pilot by 2021, I believe.
Q. Are you aware whether Georgia has already conducted a pilot risk-limiting audit of any kind?
A. Yes. On the county level.
Q. And you're aware of the Georgia statutory requirement that an audit be performed of the November 2020 election, correct?
A. Yes. Though, not a risk-limiting audit. So there is potential arbitrary risk that the audit could fail to detect outcome changing fraud.

Q. But it is possible that Georgia may choose to conduct a risk-limiting audit in November 2020, correct?
A. I suppose it's possible that Georgia could make whatever changes it wants to its election system between now and November.
Q. The reason I ask is -- and, again, I'm not asking for your legal opinion on this. But is it consistent with your understanding that the requirement for November 2020 is there must be an audit but not requirements beyond that?
A. That's consistent with my understanding.
Q. If you could turn to page 61 of the recommendations. The first bullet there indicates that states -- well, I guess it's recommendations about grant funds. But it recommends improvements in cybersecurity like hiring additional IT staff, updating software, contracting with vendors to provide cybersecurity services. Is it your understanding those things are happening in the State of Georgia related to elections, or do you know?
A. It's my understanding that those are happening to some extent. But you can tell from the way that this is written that it's not simply a box to be checked. These words mean -- these words imply a large range of activities that if done with sufficient diligence

will help, but it's more than simply having hired someone.

Q. All right. So next I want to move to some of the work that you've done in the public space. I'm using this next exhibit as a placeholder to talk about the New York Times video.

(Exhibit No. 9 marked.)

BY MR. TYSON:

Q. So let me hand you what we've marked as No. 9. And this is a printout of New York Times story titled I Hacked an Election. So Can the Russians. A video of a part of a series on voting in America. Do you recall participating in this video series for the New York Times?

A. Yes, I do.

Q. And can you describe generally what the videos in this series involved?

A. I actually haven't seen the other videos in the series. So I can only tell you about the video that I participated in.

Q. We'll start with yours then. Why don't you tell us about that video that you participated in?

A. Right. So that video was about risks to election security that involve attacks on voting machines and the potential for malicious software on voting

machines to change the way votes are counted.
Q. And were you approached by the New York Times, or did you approach them to create this video?
A. I was approached by them.
Q. Okay. And it's fair to say that the focus of the video you participated in was to bring attention to your area of research, correct?
A. Was to bring attention to the risks to elections that my research touches on. Yes.
Q. And ultimately bringing attention to that was part of the goal to influence policymakers to abandon electronic voting systems?
A. Well, to influence general improvements to election security. That's right.
Q. And one of those improvements to election security would be abandoning electronic voting machines without a paper trail, correct?
A. Well, would be -- would be adopting machines that are able to generate evidence where that evidence is actually reviewed sufficiently in order for risks of the equipment being hacked no longer to be a concern.
Q. We talked earlier about the ethical implications of certain types of hacking, hospitals and those kinds of things. Have you done any research or published any research or given thought to the ethical

implications of saying elections could be hacked and what that may mean for our system of government?
A. Yes, I have given attention to that.
Q. Have you published any papers on that topic?
A. Yes, I have.
Q. And could you point me to those in your CV?
A. There's a paper entitled ethical implications of electronic voting research or something like that, which if you'll give me a copy of my CV, I can point you to.
Q. It's actually Exhibit 2.
A. Thank you. Oh, is that attachment to Exhibit 2 here.
Q. Yes.
A. Oh, where is that? It would be reference 82 on page 57 of this document, page 13 of the CV.
Q. And I'm assuming in that paper you've concluded that it is ethical to discuss the security of election systems, correct?
A. It's a long discussion of various scenarios, but we do touch on that topic, I believe. It's been a long time.
Q. Now, in addition to your New York Times video, you've also written an editorial in The Washington Post about election security, correct?
A. That's right.

Q. I'm going to hand you what we've marked as Exhibit 10.

(Exhibit No. 10 marked.)

BY MR. TYSON:

Q. And I'll ask if that's your Washington Post editorial.

A. Yes.

Q. And if you could turn with me to the fourth page there. The top of that page begins one simple answer is that lawmakers need a straightforward policy agenda to fix the system.

So you were offering up a policy solution that was recommended by your research; is that fair to say?

A. Well, so my research coupled with the political and legislative dynamics.

Q. And what political and legislative dynamics are you referring to?

A. Well, so this is recommending federal policy, and there are certain questions about what's the strongest level of security recommendation, for instance, that would be likely to be passed by the congress and signed by the president. So it's possible that the political compromises involved there will result in a solution that's less than

perfectly effective.
Q. So you were advocating against or kind of in favor of more secure voting systems and made these recommendations based on what you thought was a reasonable path forward politically; is that fair to say?
A. Or a plausible path forward politically in part.
Q. Okay. And so those recommendations include the second paragraph there, replacing paperless voting machines with systems that include a good old fashioned paper ballot.
A. Indeed.
Q. And you personally believe that the best system would replace paperless DRE machines and be a good old fashioned paper ballot, correct?
A. I do, in the sense of a ballot that is hand-marked by those who are able to.
Q. And you also wrote an article on the online platform Medium about hacked elections in 2016. Do you recall that article?
A. I do.
(Exhibit No. 11 marked.)
BY MR. TYSON:
Q. So first of all, the reason for the article indicates you wanted to set the record straight about

something. Let me hand you what we've marked as Exhibit 11. I'll ask you first is that the article that you wrote on Medium?

A. Yes.

Q. Okay. So on the first page there, you indicate that you wanted to set the record straight about what you had been saying to the Clinton campaign and everyone else who's willing to listen; is that right?

A. That's right.

Q. And so what record needed to be set straight?

A. Right. So there had been an article in New York magazine that incorrectly attributed to me -- and this is in the immediate aftermath of the 2016 election -- the view that I suppose that I thought that the election had been -- result had been changed my hacking.

Q. Okay. So on the second page then, underneath the map, if you want to turn to that second page, there's a statement in that paragraph right under the map, were these year's deviations from pre-election polls the result of a cyberattack? Probably not. I believe the most likely explanation is that the polls were systematically wrong, rather than that the election was hacked.

A. That's right. At the time I think I would have said

I think there's only, say, a 20 percent chance that the result had been changed due to hacking of election systems and an 80 percent chance that it was due to the polling differences, but the implication is a 20 percent chance is still pretty high and someone probably ought to check.

Q. And today do you still believe that kind of 80/20 possibilities of what resulted in the 2016 election results?

A. No. I think that there was substantial more evidence in favor of the election result being correct that was gained because of the recounts that were partially completed in Wisconsin and Michigan.

Q. So if you could turn over to page 4. The bottom of that second paragraph before the headline in the next section you say that many states continue to use machines that are known to be insecure, sometimes with software that is a decade or more out of date, because they simply don't have the money to replace those machines. So would you take the position that a state that did not replace its machines was intentionally trying to make its elections vulnerable?

A. Well, it depends on -- it depends on the circumstances. And I think here and in other places

where I am writing about states needing to replace their machines, one thing that you'll see I keep doing is mentioning that states need more funding, and that is one of the policy goals that I've consistently supported helping to make sure that states like Georgia were getting additional funding.

Q. So this was part of the effort -- the overall advocacy effort to move away from more insecure machines, get federal funding, help states see the need. Fair to say?

A. I think my policy recommendations in those terms have been consistent.

Q. And then in the next -- the third paragraph under the headline, you mention that we use two main kinds of paper systems in the US. And you reference first a hand-marked paper ballot and second, a system that prints a record on a piece of paper. And so that would refer to -- I'm sorry. And then at the end of the paragraph, you indicate that there's a record that can't later be modified. So at this time, were you still advocating for ballot marking devices, or was this still just only a subset for disabled voters?

A. I certainly wasn't advocating for ballot marking devices. But I think the keyword in that assessment

is can't later be modified and the risk with many ballot marking devices is that the record might be modified before it gets printed and not noticed by the voter. And it's the same with VVPAT systems.

(Recess taken.)

BY MR. TYSON:

Q. All right. Dr. Halderman, I'm going to hand you what we've marked as Exhibit 12.

(Exhibit No. 12 marked.)

BY MR. TYSON:

Q. And this is a profile in apparently Michigan Alumnus magazine.

A. Oh, yes.

Q. Have you seen this before?

A. I have, yes.

Q. So I'm assuming you were interviewed for this publication.

A. I was.

Q. So if you could look with me at the first -- I'm sorry, the second page titled Hacking the Vote, It's Easier Than You Think.

A. Yes.

Q. Then the subhead line indicates that professor J. Alex Halderman has made a career studying electronic voting security. His research has changed

the concept of stolen elections from theory to reality. Would you agree with that assessment that elections have actually been stolen?

A. Well, of course elections have been stolen.

Q. Through hacking electronic voting machines?

A. I think it's probably true that there have been elections that have been altered as a result of a cyberattack. I can't point to one that successfully was because if it was successfully altered, we probably wouldn't know about it.

Q. Okay. Can you point to an unsuccessful example?

A. Yes.

Q. What is that?

A. Well, one example is the 1994 election of Nelson Mandela in South Africa where votes were tabulated by electronic means. And according to the UN and other officials who were there at the time, somebody successfully hacked into the computer network where voters -- votes were being counted and attempted to disadvantage Mandela's party, and that was detected. But the interesting thing is the election officials swore everyone to secrecy, and it wasn't until around the time of Mandela's death that some of the international officials involved started writing about it in their memoirs.

Another example would be the 2014 election in Ukraine where attackers linked to Russia reportedly attempted to -- reportedly did compromise the election reporting system and rigged it to report the wrong outcome, and that was apparently only detected in the nick of time.

Q. So let me rephrase my question then. Are you saying that any election in the United States has ever been stolen through a hack of an electronic voting machine?

A. I can't point to a specific one. But again, I think there's substantial risk that one has that we don't know about.

Q. But sitting here today, you can't identify a single election in the US that has had the result changed through a hack of electronic voting systems?

A. No. Although, as I say, we probably wouldn't know. That's one of the problems with electronic voting systems.

Q. If you could turn to page 9 of this profile. And that first full paragraph begins with -- let me just read it. The only reason there's no evidence of whether voting machines or vote tabulating equipment was hacked in the 2016 presidential election, Halderman insists, is because nobody allowed him or

anyone else to check. And that's consistent with what you've described earlier in terms of not being able to do full recounts or analysis of electronic voting machines after the 2016 election?

A. Well, it's also referring to forensics on voting systems and so forth. Yes.

Q. And so is it your testimony that there is evidence that machines were hacked, and that if you looked, you would find that, or you just don't know?

A. If machines were hacked, there's a possibility that evidence could be found by doing forensics of individual machines. That's my testimony.

Q. Okay. And the next sentence begins, this is the core of his advocacy regarding electronic voting machines and vote tabulators. Would you agree with that description of you as an advocate regarding electronic voting machines and vote tabulators?

A. I suppose it depends what you mean. I certainly do recommend specific policy measures that are necessary to secure election systems.

Q. The next page over, one, two, third full paragraph, it talks about your preparation process for testifying to the US senate committee with a murder board. Always a delightfully-named function.

A. Indeed. I'm not seeing where you mean.

Q. Right about in the middle of the page, third full paragraph.
A. It begins it was remarkable?
Q. Yes.
A. I see. Yes.
Q. And the last sentence of that paragraph says, the aim was for Halderman to avoid seeming partisan. Is there a concern that election security issues are a partisan issue at this point?
A. They're certainly a non-partisan issue at this point, as I think you can see by the broad bipartisan support in congress for things like the Secure Elections Act and the bill that Mark Meadows introduced to adopt very similar protections. But there's always a risk in discussion of elections that partisan politics will come into play.
Q. But at this point, you are not aware of partisan politics around the adoption of hand-marked paper ballots?
A. I was aware that -- I was aware, and I believe there still is a risk that partisan politics will -- will override the very real technical issues and make it difficult to have strong security legislation.
Q. Are you aware of the partisan breakdown of votes in the Georgia General Assembly about hand-marked paper

ballots versus ballot marking devices as an election system?

A. No, I'm not aware.

Q. Would it surprise you if those were partisan votes?

A. I think most votes are pretty partisan.

Q. So it wouldn't surprise you?

A. So it wouldn't surprise me. Although, I'm not sure which way the partisan politics would work out in this particular issue in Georgia.

Q. Going up that page just a little bit. We talked about your Medium essay, and this is a portion discussing that. You indicated that after you wrote your Medium essay, you had come to a point of greater confidence that the polling information was wrong versus the election was hacked based on the partial recounts that were conducted. On that third paragraph there, it indicates that the effort to conduct recounts didn't succeed, and recounts were only conducted in Wisconsin with minimal changes and nobody was able to inspect any of the equipment.

What is it about the recount process that changed your view from your Medium essay to now about the 2016 election?

A. That the recount involved in large parts of Wisconsin and in parts of Michigan involved manual inspection

of ballots that had been marked by hand served to provide additional evidence for the correctness of the election results and that those manual inspections of hand-marked records didn't reveal a systematic deviation from the reported results.

Q. There's also a reference in that paragraph that on cable news and social media, you were dubbed a Stein puppeteer trying to steal the election for Hillary Clinton. Is that an example of the partisan politics that you discussed that could enter into those questions?

A. Yes. I think that -- that experts being labeled partisans merely because their views are inconvenient for the views of a political group is a substantial part of the risk.

Q. There's also a great account in this article about you meeting a man in a trench coat to obtain a contraband voting machine. Do you recall that event?

A. I do.

Q. And do you recall what kind of voting machine that was?

A. It was an AccuVote TS DRE.

Q. That's the kind used in the State of Georgia up until the end of 2019, right?

A. That's correct.

Q. And on page 5 is where I am. It's not necessarily relevant. It just mentions that you posted a video about -- of the machine being hacked in a mock election between Benedict Arnold and George Washington. Is that the same hacking demonstration you performed for Judge Totenberg in 2018?
A. I performed a similar demonstration.
Q. But it wasn't the same type of hack demonstration?
A. No. Actually, it was using a different but also effective way of hacking the AccuVote TS and TSX.
Q. Okay. And the demonstration that you did in the YouTube video, would that have been untraceable to someone looking at the voting machine? Just in terms of the main files, if they didn't dig into the system architecture and just reviewed the reported files, would that have been detectable in any way?
A. No, it wouldn't have been detectable.
Q. And just to stick with the 2016 recount piece for a moment --
A. You mean the Michigan Alumnus piece?
Q. I'm sorry. No. Just the concept of doing recounts following the 2016 election. Not the exhibit. We're finished with the exhibit.

You assisted with the efforts to obtain recounts in Michigan, Wisconsin, and Pennsylvania in

2016; is that right?
A. Yes.
Q. And were you retained by the Stein campaign or the Clinton campaign?
A. I was retained by the Stein campaign.
Q. And did you assist with recounts in any other states in 2016?
A. No, just those three.
Q. And all three of those states were won by President Trump in 2016, correct?
A. Yes. That's correct.
Q. And were these efforts you undertook pro bono, or were you being paid by the campaign?
A. I was being paid.
Q. Have you ever worked as a staffer on any political campaign?
A. No, I haven't.
Q. Have you ever been retained by political campaigns beside the Stein campaign?
A. No. Oh, actually, strike that. Yes, I have. I have on one other occasion.
Q. And what campaign was that?
A. That's the current political campaign for the presidency of the Dominican Republic.
Q. So I can clarify that quickly. In the United States,

you've not been retained by any other candidate or campaign?
A. No.
Q. Okay. Now, you hold at least one patent; is that correct?
A. Yes, that's correct.
Q. I want to hand you what we've marked as Exhibit 13.
(Exhibit No. 13 marked.)
BY MR. TYSON:
Q. I'll ask if this is a patent that you hold as an inventor.
A. Yes, it is.
Q. And what does this patent involve?
A. This is a system for efficiently auditing elections by using a high-speed scanner to review electronically paper ballots and then using statistical sampling similar to an RLA to confirm the results.
Q. Now, do you retain any financial interest in the use of this patent going forward?
A. No. In fact, Princeton has dedicated it to the public domain at my request.
Q. If you could turn to the -- I guess it's the one, two, three, fourth, fifth physical page. The top begins System and Method For Machine-Assisted

Electronic Auditing.
A. I'm sorry. Can you repeat the page?
Q. Sure. The fifth physical page.
A. The fifth -- the marked column 5 here?
MR. HERMAN: The actual.
BY MR. TYSON:
Q. Yeah. The actual fifth page.
A. The pages I don't think are numbered.
Q. Oh, I see. The columns are numbered. My apologies. I'm not a patent lawyer. If you could look at column 2, down where line 25 is.
A. Yes.
Q. There's an indication that the primary weakness of a particular method you're referring to and discussing is establishing a link between electronic and paper ballots at the time votes are cast. Is this issue of voter privacy, that if we kind of sequentially number every ballot as it's collected and could tie that back to voters that are voting at particular times a common issue you encounter in the design of audits for election systems?
A. Excuse me. Let me just review those two paragraphs.
Q. Certainly. Yes.
A. Yes. Sequential numbering of ballots is a common issue in audits and in the design of voting systems

more generally and creates privacy risks.
Q. The way I've thought about it is I've tried to think about it in the past. If we could maintain the link between the person and the ballot, auditing would probably be pretty simple I'm guessing at that point. We could use some sort of log method for that. But the importance of the secret ballot that we have to separate those two pieces of information, is it correct to say that's what leads to a lot of the challenges around how we handle ballots and how we do audits?
A. I would say that, more broadly than that, that the need for a secret ballot complicates much of election security.
Q. Okay.
A. If we could just print everyone's name and vote in the newspaper, it would be much easier.
Q. From a security standpoint, but not from a constitutional or administrative standpoint, correct?
A. In fact, it would be bad from a security standpoint too because the secret ballot is an important defense against certain attacks.
Q. So printing everybody's votes in the newspaper would help with some attacks but would lead to other possible attacks. Is that what you're saying?

A. That's right.
Q. So in the election field, do you consistently find these kinds of trade-offs, that doing one thing may solve one problem but create a host of other problems?
A. That's right. That's why we need to be -- that's why only certain technological approaches achieve a high level of security all around.
Q. But you'd agree with me that if, for example, the United States of America decided that the secret ballot was no longer an important consideration as just a policy matter, that would change the mix of technology in what we used going forward, right? I know that's a wild hypothetical.
A. That's a wild hypothetical. If it was actually true, contrary to reality, that the secret ballot wasn't important, it would be easier to design secure election systems.
Q. Just out of curiosity, I'm sure you followed what's happened with the Iowa caucuses.
A. I have.
Q. Is it possible there's some kind of hacking for that system, or do you have -- have you done any research or have any opinions about that system?
A. On the Iowa caucus system? What part of it do you

mean?
Q. I'm only going on news accounts that there have been problems with the tabulation and an app that was being used.
A. Right. Do you have a specific question?
Q. It was just my own personal curiosity. We can move on. Sorry.
A. What a mess. Let me just say what a mess.
Q. All right. So it's fair to say that you believe electronic voting brings a host of problems to the election system; is that fair to say?
A. Yes. It exposes the election system to several different kinds of attacks.
Q. Is there any circumstance besides disabled voters where you would support the use of electronic machines over hand-marked paper ballots?
A. You mean ballot marking devices over hand-marked paper ballots?
Q. Any type of electronic ballot marker, whether done through a DRE, through a ballot marking device, any scenario.
A. I see. Is there any scenario? In general, no.
Q. So are you thinking of something besides disabled voters where you might be willing to support electronic voting?

A. Well, I'm thinking, for instance, in some extreme emergency, would it be -- would I be -- would I say I would support it? Well, it's hard to say. It really depends on the facts of the situation.

Q. And it's fair to say that setting aside disabled voters, you believe that hand-marked paper ballots that are fully audited is the best method of administering elections, right?

A. I think from a security perspective, that's correct.

Q. From an administerability standpoint, do you not think that's correct, or is there a perspective where you would disagree with that? The reason why I ask -- I can clarify. I know you're trying to figure out what I asked.

You clarified your answer with that you believe from a security perspective that hand-marked paper ballots with full audit to be the best method of administering elections. So my question is why only from that perspective.

A. Oh, I see what you mean. There are -- there may be administrative reasons to prefer other systems in certain circumstances. Although, I think the alternatives do create a large and uncovered risk of attacks to the election system.

Q. So there may be policy reasons for using some

electronic components, is that what you're saying, but it creates a security risk in the process?
A. Yes.
Q. I'm assuming that you don't believe that hand counting all ballots is the best possible system.
A. That's correct.
Q. And why is that?
A. Because hand counting all ballots -- hand counting all ballots would take a very long time. Hand counting we know also creates its own set of security risks.

My perspective is that the best way to administer and secure elections is to count ballots electronically, but to confirm the results of the electronic counting through manual follow-up.
Q. So if we had a system that involved hand-marked ballots that were hand counted, would you still think audits were required in that scenario?
A. Some kind of audit I would say would still be required. But it wouldn't be the same kind of audit that would be an RLA, for instance, designed to specifically detect errors in a machine count because you wouldn't have a machine count.
Q. And when you mentioned that hand counting can bring other challenges, would that include election

officials overvoting a ballot, for example, during a hand count?

A. That's a potential risk. If the election officials are dishonest, they could potentially make changes to the ballots during counting. That's right.

Q. And you think it would be best for the State of Georgia to have a system of hand-marked paper ballots as the primary means of voting, right?

A. Yes, I do.

Q. I'm going to change direction a little bit. Are you good to keep ongoing?

A. Yeah. Let's keep on going a little bit. I assume we're thinking of lunch at some point.

Q. Eventually, yes. Probably have a good stopping point here in a little bit.

I want to talk about some general things about your report, Exhibit 2. If you want to get that in front of you. Talk about some high level pieces to it first, and then move through some of the specifics.

All right. So through your report, is there a particular section of your report that summarizes the opinions that you offer in it?

A. I'm not sure there's a particular section that does.

Q. If you could go with me to paragraph 20. When I was

looking for it, it seems paragraphs 20 and 23 seems to summarize things well. If you want to get there, it's on page 6 on the bottom, 7 on the top.

A. Okay.

Q. So in this -- in paragraph 20 to start with, you identify your opinion about a variety of scenarios of what could happen based on Georgia's election system facing a high risk of being targeted. Is that a fair statement?

A. Yes.

Q. So you say, first sentence, that there's a high risk of being targeted by sophisticated adversaries. Second, those adversaries could attempt to hack the election system. Third, they could sabotage BMDs or optical scanners. Fourth, they could infiltrate BMDs and optical scanners. And fifth, those attacks could succeed despite efforts that Georgia has put in place.

Is that a fair list of things that you think are the main problems from Georgia's perspective?

A. With the new system, I think it's fair to say that's a good summary of much of what's in my opinion --

Q. Okay.

A. -- in my report.

Q. And you're not saying that these scenarios definitely will happen or have happened. You're just saying they might happen, correct?
A. I'm not saying they definitely will happen. I'm saying that there's a high risk that they might happen.
Q. You'd agree with me that every election system used by every state is subject to the potential targeting by sophisticated adversaries, right?
A. Yes. That's why in every election system in every state things like hand-marked paper ballots and risk limiting audits are an important defense.
Q. And you'd agree with me that every election system used by every state has the potential to be hacked, right?
A. Indeed. Again, that's why these protections are so essential.
Q. And you'd agree with me that attackers could sabotage components of the election system used in every state, right?
A. That's right. Again, why these defenses are so important.
Q. And you'd agree with me that attackers could place malicious software on BMDs or optical scanners in the election system of every state, right?

A. Where those components are used, that's right. Very few states use BMDs for all voters.
Q. But all states use optical scanners, right?
A. At least somewhere. Not in all jurisdictions in all states unfortunately. There are still some paperless jurisdictions.
Q. And you'd agree with me that the kind of attacks that we've outlined here could also succeed in other states too, right?
A. Yes.
Q. So in approaching your opinion about Georgia's election system, what kind of specialized knowledge are you using to come up with these potential scenarios if they could apply to every states' election system?
A. What do you mean by specialized knowledge?
Q. Does it require any special training or experience to be able to outline the scenarios you've outlined in paragraph 20?
A. Yes. Yes, it does.
Q. And what -- I'm sorry. Finish.
A. Yes, it does. So I've been studying security risks to electronic voting systems for getting close to 20 years now. And so I think that kind of specialized knowledge is important in assessing both the threat

and the level of risk.
Q. And so you do have specialized knowledge about kind of the potential vectors of attack, I think as we refer to them, on computers that are used in the election system. Fair to say?
A. Yes.
Q. And your focus has been primarily on the cyber vulnerabilities of an election system, the computers that are involved, not on the potential manipulation of paper ballots through kind of old school methods. We've referred to overvoting a ballot, for example. Your research is focused primarily on the cyber risks, right?
A. I would say primarily. But it also considers those other risks, and I teach about them. And auditing or other defensive methods that I talk about are designed with those risks in mind too.
Q. So in reaching your opinions about Georgia's election system, you are evaluating all the potential risks, not only the cyber risks but also other possible security risks?
A. Well, I have thought about other potential security risks, but the opinion here is primarily about the risks of cyber attacks.
Q. And in reaching your conclusion about Georgia's

election system facing a high risk, is that including the other security risks beyond cyber, or is that limited to a cyber risk for the State of Georgia?

A. Here I'm talking about the risks of attack by sophisticated adversaries like hostile governments in the context of attacks on computer system.

Q. Okay. And so in reaching your opinions in your report, you've obviously used your specialized knowledge to come up with a series of scenarios of things that could happen. And then you're assessing how likely or unlikely those scenarios are to happen, or are you just identifying these are possible attacks?

A. I'm also assessing the level of risk.

Q. Okay. And have you ever evaluated comparative risks of an entirely paper ballot election system versus a system that uses some electronic components?

A. Of an entirely -- you mean a hypothetical?

Q. Excepting disabled voters. A hand-marked paper ballot system for the comparative risk of that system versus a system that uses electronic components.

A. I have evaluated the risks in hand-marked paper ballot systems, including for the Secretary of State of Michigan. So yes.

Q. And what is the method you've used to evaluate the

comparative risks of those types of systems? If you're trying to compare one system's risks with another, what is the method you'd used to evaluate that comparative risk?

A. So the method is basically what are -- examining the differences between those voting systems and which new attack vectors they make possible and how likely are those vectors to be exploited.

Q. So you essentially say okay, for system one, let's say hand-marked paper ballot system with ballot marking devices for disabled voters, electronically tabulated using optical scanners, here's the list of possible risks we face with that system?

A. Of cybersecurity risks and which ones are enabled by this change of technology.

Q. And then we look at a system, ballot marking device system for all voters, what are the risks with that system. So my question is, how do you then decide which system is more or less secure based on that list of risks? Is there a specific method you use for that?

A. Sure. So, for instance, in the ballot marking device study that I published in January, we have a quantitative method. There was an equation in there that will tell you based on the proportion of voters

who are using a ballot marking device versus a hand-marked system, what is the additional risk that's created by -- that outcome changing fraud will go undetected.

Q. And that's specifically related to voters verifying their paper ballots, right?

A. Right. Which is one of the very significant defenses in an election system is voter verification. That's the premise of BMD security, that voters will successfully verify.

Q. And it's not your testimony that there exists one perfectly secure voting system, right?

A. There are voting systems that have greater or lesser risk for certain important categories of attacks and ones that have no risk of certain categories of attacks. So I think the -- which is more secure or not is pretty clear.

Q. You say which is more secure or not is pretty clear. Would that be as to overall policy reasons for one system or another, or which one is more or less secure from a cybersecurity standpoint?

A. Well, I'm speaking specifically from a cybersecurity standpoint.

Q. And as we covered earlier, there are scenarios where policymakers may have interest beyond cybersecurity

in selecting a particular election system, correct?
A. There are other interests that come to play. I believe that there -- but I don't think that the other interests, as they are practically manifested, outweigh the cybersecurity advantages or disadvantages that are part of that equation.
Q. And you've gotten where I was trying to get to earlier. So then what is the way that you determine whether the other policy reasons outweigh the cybersecurity risks?
A. Well, we could talk about that in the context of specific policy questions that are coming to bear. The question is to me the methodology that I would apply is what are the alternative ways of achieving this policy goal and are there practical cybersecurity techniques that we could use to achieve security under those circumstances. And when the outcome turns out to be no, we either have a system that is at high risk of attack or not, I think that the policy -- the policy balance outcome is pretty clear.
Q. And, again, the methods you're using to make that policy balance outcome that you see is so clear is you are looking at possibly alternative policies that could have less cyber risk; is that a fair way to say

that?
A. Well, possible -- can you repeat the question?
Q. Sure. I'm just trying to understand how you weigh the policy options of the other policy reasons why a jurisdiction may have for other systems versus the cyber basis. And particularly I'm looking for what method are you using to conclude that hand-marked paper ballots are the right election system to be used. You're reaching a conclusion they are.
A. I see.
Q. That's what I'm trying to understand. What method are you using for that evaluation?
A. There's a very stark cybersecurity difference between the hand-marked system and/or hypothetical or not hypothetical BMD for all system. And so given the sort of starkness of that contrast, the question is can you achieve those same -- the question to me is can you achieve the same policy objectives well with the hand-marked system. Right? And if you can achieve those policy objectives well with the system that is significantly more secure, then I believe on the basis of that reasoning it's the -- it's the superior choice.
Q. And it's a policy interest of a state, is it not, to have voter intent be clear? Could that be a policy

interest for a state?
A. That could be a policy interest.
Q. And in that policy interest, you'd agree with me that ballot marking devices are superior to hand-marked paper ballots, right?
A. Not necessarily. So hand-marked paper ballots. You can also have the optical scanner reject ballots that the scanner determines are not clearly marked, and that's a feature of the Dominion system, in fact.
Q. And in those scenarios, have you ever talked to election officials about what voter behavior happens when a scanner rejects an improperly marked hand paper ballot?
A. I have talked to election officials about that, yes.
Q. What have they told you?
A. Some election officials have told me, in fact, that when -- some election officials have told me that they worry about delay that's caused by that scenario. But other election officials have told me that they already have their scanners programmed to work in that way and it's fine.
Q. And election officials may have concerns about voters becoming frustrated in the process. Have you heard that from election officials?
A. I've heard that about BMD-based elections as well as

hand-marked elections. So that is a concern either way.

Q. And those would be other policy interests that might underlie the selection of one system over another unrelated to cybersecurity, correct?

A. There are other important considerations.

Q. So you'd agree with me that it's not possible to eliminate every attack vector against an election system, right?

A. Not every attack vector. I mean, someone could cut the power to the entire state somehow and just render absolute chaos. But in terms of attack vectors that involve -- that involve hacking the computer systems that are used to administer the election or that are in the polling place, it's possible to reduce the risks to a minimal level.

Q. And when you say reduce the risks to a minimum level, how are you categorizing minimal risk versus other types of risk? What method are you using to arrive at this is a minimal risk system?

A. Well, let me be more clear than that. It's possible to eliminate the risk that hacking polling place equipment is going to be able to change the election outcome or cause significant disruption through a well-designed system.

Q. But it's not possible to eliminate all the risks. I think we talked about earlier every election system is subject to being targeted by sophisticated adversaries. Every election system could have some components of it hacked. Every election system could have software put on optical scanners. So I guess I'm trying to understand where you're concluding there's minimal risk if there's always going to be these vulnerabilities for any election system.

A. Well, at the point where we can have a high and quantifiable statistical probability of detecting and correcting attacks of that form, I would say the risk has been well constrained.

Q. And ultimately, though, isn't that a policy decision of what level of risk someone is willing to encounter?

A. Well, it's a policy decision -- is it a policy decision? Can you repeat the question?

Q. So we're talking about all these different interests that go into elections. You can reduce it to a statistically quantifiable number that we can have confidence in a particular outcome. But maybe in the process, we're going to create long lines to do that. There's all these competing policy interests in the space of the design of an election system. So what

I'm trying to get to is at what point is it a policy decision and at what point is it a scientific process you're using to arrive at your conclusions in this report.

A. Well, I reject the notion that it's actually a trade-off between long lines and good security. But, I mean, if there's a policy decision that we would like the election system to be at high risk of attack by foreign governments, I suppose that is a policy decision too, but I don't think it's a policy decision that I as someone who is an expert in election cybersecurity would get behind.

Q. Do you use online banking?

A. I do.

Q. And I'm sure -- I do too. And there are risks, of course, that online banking is subject to manipulation, hacking, targeted by foreign powers, right?

A. Yes. And, in fact, there are billions of dollars of fraud every year reportedly in the financial sector due to hacking.

Q. But obviously you've chosen, I've chosen to use a system that has some risk for the sake of convenience; is that fair to say?

A. Well, I think the risks in online banking are fairly

well constrained for consumers because of things like FDIC protection, and most fundamentally, because if the money is gone, we're going few notice. The same can't be said unfortunately of election systems. If the result is wrong, it's not necessarily going to be apparent to anyone.

Q. And I believe I saw you have a cellphone.

A. I do. It's right here.

Q. I do too. And cellphones are subject to manipulation, hacking, targeting by foreign powers, right?

A. Potentially.

Q. And yet, we use those because we've chosen to encounter a degree of risk for the sake of convenience, right?

A. Well, so, again, if my cellphone is hacked, we won't -- that will not end up causing something like a national election outcome to be wrong, I hope. But there are good reasons, including the vulnerability of cellphones, that we don't, for instance, let you vote using an app on your cellphone in elections in Georgia. That's because the risks are substantial.

Q. So I guess thinking about those examples, is your ultimate opinion in your report that Georgia policymakers have chosen to take too great a risk by

using an all ballot marking device system election system?

A. So my opinion is that it's a very, very substantial risk. And if -- and yes, I would say that the process in Georgia that has led to this risk has resulted in an undesirable outcome from the perspective of protecting the votes of the people of Georgia.

Q. So it's your opinion that Georgia policymakers have chosen a path with too much risk to use for elections, right?

A. Yes, I think it's too risky a path.

Q. And that opinion lines up with your personal views on election administration, right?

A. With my personal views? How do you distinguish from my professional views in this case?

Q. I believe you said earlier that you believe the best system for administering elections is a hand-marked paper ballot system with ballot marking devices for disabled voters.

A. I see. Yes, I think it's consistent with that. It's totally consistent with that, yes.

Q. And so what scientific method are you using to determine that Georgia policymakers have taken a path with too great a risk? There's obviously a point

that you cross over a threshold. What method do you use scientifically to determine where that tipping point is?

A. Where that tipping point is? Oh, I see. Well, I think the -- I think the tipping point -- that question, it comes down to a -- it comes down to applying the expertise that I have from evaluating voting systems to ask the question, is this system actually going to provide a strong defense or not. And so there's -- it's a matter of -- it's a matter of comparatively assessing those risks.

Q. Are there published studies about evaluating acceptable degrees of risk in the election context?

A. Probably there are. So if you look at, for instance, the California top-to-bottom review studies that were commissioned in 2007, those studies technically are focused on vulnerabilities in specific pieces of election equipment but come out with the policy recommendation that they not be used because the risk is unacceptable.

Q. And that was a policy recommendation as the result of that analysis, correct?

A. That's right.

Q. So you have the California top-to-bottom review. Have you ever published papers on determining what

the acceptable degree of risk in election systems is?
A. Acceptable degree of risk.
Q. And the reason why I ask is, again, you're saying that Georgia policymakers have taken too much risk. So how -- have you ever published a paper evaluating the acceptable degree of risk?
A. So the ballot marking device paper that I published in January tries to assess some of that in part by trying to quantify whether -- whether in a given system attacks are going to be detected or not, what's the probability that an attack would be detected. If the system is achieving an acceptable degree of risk, that probability is going to be high for plausible attacks. If it's not, it's going to be low. You can indeed quantify some of these things.
Q. Did you determine the exact percentage at which you cross that threshold in your study of ballot marking devices?
A. No. But it's quite often the case in science that rather than a clean threshold, you just have a breakdown between scenarios that result in a low output value and a high output value.
Q. And so beyond the BMD paper, you can't think of any other papers you've published looking at the acceptable degree of risk in an election system?

A. I think that's the most quantitative one.
Q. But you can't think of any others?
A. Not off the top of my head. But I have published a lot of papers in this area, so it's quite possible.
Q. Sure. Is the field of determining an acceptable degree of risk in non-election context, are you aware of that being a discipline that people study what -- when people encounter certain degrees of risk?
A. That's quite often a question that comes up in matters of public policy and science.
Q. But you didn't rely on any papers outside the election context about assessing acceptable degrees of risks in forming your opinions in this report, right?
A. No, I didn't.
Q. A couple other global questions, and I think we'll probably be at a good stopping point for lunch. We'll dig into the details of the report after that.

Kind of globally throughout the report there's terms potentially, possibly, could happen. There's a lot of scenarios of what might happen along the way. And I believe we covered this already. But you are not aware of anyone who's ever documented an actual compromise of an election system using electronic voting equipment in an actual US election,

correct? And I know I added a bunch of qualifiers on there.

A. You mean a hostile compromise?

Q. Any compromise --

A. Any compromise?

Q. -- in a US election system of an electronic voting machine.

A. Sure. There are plenty of voting machines in US elections used in US elections that have been actually demonstratively compromised.

Q. And what are some examples of those?

A. The previous voting machines used in Georgia, the TS and TSX that I personally compromised, those kinds of machines.

Q. My question was that were being used in an actual election.

A. Those machines were used in actual elections in Georgia from 2002 until 2019.

Q. What I'm trying to get to is not a machine generally, a model type that is being used in an election, but an actual machine in a precinct on election day in a US election.

A. I see.

Q. Has anyone ever documented a case of one of those machines ever being compromised?

A. I don't believe so.
MR. HERMAN: Okay. Off the record for a second.
(Recess taken.)
MR. TYSON: Back on the record.
BY MR. TYSON:
Q. All right. Dr. Halderman, before lunch, I said we were going to turn to your report. I apologize. I do have one more thing I wanted to ask before we go there.
A. Yes.
Q. You're on the board of advisors for the Verified Voting Foundation; is that right?
A. I am.
Q. And can you briefly describe what the Verified Voting Foundation is.
A. The Verified Voting -- the Verified Voting Foundation is a group that advocates for stronger election security.
Q. And when you say stronger election security, is it primarily the cybersecurity component that you -- the field that you work in?
A. Yes. Primarily. It's a group that was founded originally by computer scientists, and that's the focus of their activity.

Q. Got it. Were you involved in developing the principles for new voting systems from the Verified Voting Foundation?
A. I don't think so. No.
Q. Okay. I'm going to hand you what I've marked as Exhibit 14.
(Exhibit No. 14 marked.)
BY MR. TYSON:
Q. Have you seen this document before?
A. Yes. Well, actually, wait. No. There's a new set of principles since -- since 2015, I believe.
Q. Okay.
A. Or a new set of positions that I have seen, but I don't think I've seen this version.
Q. And this is the one I got off the website. So I might have gotten the wrong one.
I wanted to ask about a couple of these principles. So No. 1, the system should use human readable marks on paper as the official record of voter preferences and as the official medium to store votes. Does the Verified Voting Foundation, to your knowledge, accept ballot marking device ballots as a valid way of voting, or is it only hand-marked ballots?
A. I believe that their current set of -- their current

set of positions on these issues point to elevated risk with ballot marking devices.

Q. Let me ask about No. 7. One of the other principles is to use commercial off-the-shelf hardware and open-source software. Do you agree with that principle of security in voting systems?

A. Yes, I think all else being equal, that's probably something that is at least somewhat preferred, although commercial off-the-shelf hardware and open-source software can also still have significant security risks.

Q. Okay. Is there a reason just from a cybersecurity perspective to prefer commercial off-the-shelf hardware versus custom-built hardware?

A. There is a reason to prefer it. Again, all else being equal, in general, developing hardware is difficult and off-the-shelf hardware is more likely to have been well tested than hardware that is proprietary. But it really depends on the specific case whether it actually achieves security benefits or not.

Q. And does the same set of principles apply to open-source software versus I'm assuming custom-designed software?

A. Yes. Although, open-source software has the

additional benefit of making the code available to others to review, which carries with it additional security benefits since it's open to broader scrutiny for problems.

Q. And so since it's open to broader scrutiny, people could find vulnerabilities and notify whoever they need to to repair them; is that the general principle?

A. Well, that's right. And so it's -- in addition, it makes it easier to I think credibly assess the likely level of security of the piece of software. When it's closed, it can be more challenging.

Q. What is the role of kind of trade secret in voting software particularly versus an open-source approach? Are there pros and cons security-wise to each, or is one always preferred over the other?

A. I would say there are pros and cons.

Q. And can you give me some examples of what the pros of trade secret and what the pros of open source would be?

A. Well, the broader principle is that in a system that is important for security, the parts that need to remain secret for security should be well defined. This is called Kerckhoffs' principle. It's sort of a foundation principle in security. And it's easier to

achieve that in an open-source system than a closed-source sytem because in the closed-source sytem, everything is being kept secret. You might not be able to compartmentalize the pieces that need to be kept secret. But yes, there's a need to keep some secrets secret in basically any secure system. But they should be limited to things like cryptographic keys that are well defined and narrow. That's the principle.

Q. All right. Well, let's go ahead and turn to your report. And the good news, we can skip ahead to paragraph 14. So we'll start on page 3. What I wanted to do primarily, just kind of walk through the report and ask about some of the conclusions you've reached and some of the decisions or the opinions that you've offered in this case.

So first of all, you indicate in paragraph 14 that you were asked to opine on the security of Georgia's election system following the implementation of the new system. Is it your understanding that the Dominion voting system and the KnowInk system is at issue in this case?

A. Yes, it's my understanding that it's at issue in this case.

Q. And you walk through the various components of that,

the ballot marking devices, the ICX component, the ICP precinct scanners, the ICC central-count scanners. Have you personally observed and tested an ICX ballot marking device?

A. No, I have not.

Q. Have you personally observed and tested an ICP precinct-count scanner?

A. No, I have not.

Q. Have you personally observed and tested an ICC central-count scanner?

A. No, I have not.

Q. Have you personally observed and tested the Democracy Suite election management system?

A. No, I have not.

Q. And have you personally examined and tested any Poll Pad electronic poll books?

A. No, I haven't. My views on the systems are based on the experience that I've had over the last nearly 20 years with other electronic voting systems and the design of the systems as documented by Dominion and the tests that have been conducted in other states.

Q. Okay. So it's not based on any personal evaluation. It's based on your knowledge, tests of others, and understanding of the system from Dominion itself?

A. That's right.

Q. Okay. And I believe in 15 we've already covered that you reviewed the documents the plaintiffs provided to you from Dominion. Let's go to paragraph 16 about the eNet software.
A. Yes.
Q. And eNet is Georgia's voter registration database, correct?
A. That's correct. It's the software that runs the voter registration database and some associated administrative functions.
Q. Do you know approximately how many states use eNet? Is it a widely-used piece of software?
A. There are versions of eNet used in other states. I know that.
Q. Are there other voter registration database software that is more widely used than eNet, or is eNet kind of one of the main players in this space?
A. It certainly is a player in this space. But there are different versions of the software that are used in other states, some of which are relatively better protected.
Q. Okay. And have you evaluated the protection of Georgia's version of eNet versus the versions in other states?
A. So I am familiar with the -- I have personally

evaluated vulnerabilities in the MVP and OVR system compared to other states as a component of the broader eNet platform.

Q. Is it your testimony that MVP and OVR are part of the eNet system?

A. Are interfaced with it. That's right.

Q. And when you say interfaced with it, what do you mean interfaced with it?

A. I mean that data from those systems feeds into the overall voter registration system and vice versa.

Q. And does that happen without human intervention, or is there a human intervention component for either of those MVP and OVR systems to alter the voter registration database?

A. There may be a human component for the -- some of the data that's fed back in. I think the data that comes out is read out by a computer process.

Q. You say in paragraph 16 -- actually, before we go to that, you said you evaluated the MVP and OVR components. Have you evaluated the eNet version used by Georgia versus the eNet versions used by other states? For eNet specifically, not for other associated applications.

A. No, I have not.

Q. You say in the second sentence of paragraph 16 that

election officials use eNet to manage voter registration data. Which election officials use eNet to manage voter registration data in Georgia?

A. I'm not sure in Georgia's practice.

Q. And do you know which election officials export eNet data to electronic poll books?

A. I don't know. I think that happens at the Secretary of State's office. That's my understanding, but I -- but I'm willing to be corrected.

Q. In the next sentence you talk about interface of MVP and OVR and say that those systems allow voters to view and update their voter registration data. Can you explain to me how those systems update voters' voter registration data in eNet?

A. So the voter can fill in updated information through the voter -- or an updated -- or fill out a voter registration -- a voter registration form on those systems. It gets uploaded to the server. And then through back-end processes, which may or may not require human intervention, I'm not sure, the data is updated in the voter registration database.

Q. So you don't know if a voter registrar is required to review information and changes to voter registration data before those changes are made in eNet?

A. You know, I'm not sure that it makes a significant

difference to the security of the system overall. Even attacks that could affect -- attacks could affect voter registration in plausible ways that a registrar would approve.

Q. So it's your testimony that there's really no security difference whether the input of a registrar is required before changes are made?

A. It matters to some kinds of attacks, but I don't think to plausible attacks that could affect -- to certain plausible attacks that could affect the -- could affect the ability of Georgia voters to cast their votes on an election day.

Q. And then we'll come back around to that in a little bit more later on. In paragraph 17, the bottom of that page 4 you indicate absentee voters will not use BMDs. That is for people who vote absentee by mail; is that right?

A. That's my understanding.

Q. And voters who vote absentee in person, do you have an understanding of whether they will use BMDs or not?

A. I think absentee in person is a BMD process. Yes.

Q. In paragraph 18, you indicate in the second sentence that the Secretary of State will transmit the election programming files to county officials. Do

you know how that transmission is made?
A. I'm not sure whether the process has been changed from the process that was used prior to the introduction of the Dominion system or not. But the process prior to the transmission via CD ROM has significant security downsides.
Q. Okay. But you don't know the current setup that's being used, correct?
A. I'm not sure that it makes a difference for the kinds of attacks that I'm worried about. But I don't know for sure the current process. I'm not sure that that's been documented publicly yet.
Q. So it's your testimony that the method of transmission doesn't really matter to the types of attacks you're concerned about?
A. To some of the attacks I'm concerned about. That's correct.
Q. But it does matter to other types of attacks you're concerned about?
A. That's right. There can be attacks that depend on the specific method of transmission, and there are other attacks that only depend on the fact of transmission.
Q. So in evaluating the relative risks to Georgia's election system, you didn't consider the method of

transmission as informing that part of risk assessment, correct?

A. I think the method of transmission -- excuse me.

(Discussion off the record.)

BY MR. TYSON:

Q. So in reaching your conclusions about the risks faced by Georgia's election system, you did not -- since you did not know the method of transmission, you didn't take the method of transmission into account in making that assessment; is that right?

A. Well, I think that's right. The method of transmission might change the level of risk around the edges, but it's not likely to be a night and day difference.

Q. So it's not important to your overall conclusions; is that right?

A. No, I don't think it affects the overall conclusion.

Q. Okay. At the bottom of 18 you indicate that election workers will install a memory card or USB stick into each BMD and ICP scanner prior to the start of voting. Do you know which election officials or workers will do that?

A. My understanding is that in Georgia that usually happens at the county, but I'm not completely sure.

Q. Okay. And then the removal in paragraph 19 of the

memory cards for return, do you know which election workers those would be?

A. I think that happens at the polling place in Georgia, but I'm not entirely sure.

Q. And you don't mention what happens to the paper ballots after an election. Is that -- I'm assuming that's not relevant to your analysis either.

A. Well, not primarily to the cyber -- well, actually, that is something that is relevant to the analysis. I just don't mention it here.

Q. So what is the method that the paper ballots are returned back to a county official?

A. I don't know. But I'm assuming for purposes of this analysis that the paper ballots are going to be returned through an adequate chain of custody because otherwise the security situation is even worse.

Q. Okay. So then you're assuming that paper ballots are returned through an adequate chain of custody as part of reaching your conclusions about the relative risks of Georgia's system, right?

A. Well, that's right, because those risks are even worse if the chain of custody is not adequate.

Q. And since you don't know exactly who's installing memory cards, who's removing memory cards, I'm assuming that's not part of your analysis either as

far as reaching your conclusions about relative risk.
A. I tried to make generous assumptions about those risks where I don't know the answer, ones that the level of risk doesn't depend on it being the worst possible way it could be done.
Q. Again, so likely paper ballot transmission, you assumed then that qualified election workers are going to handle memory cards at all stages with the proper chain of custody; is that fair to say?
A. That's right. Even though there are still limitations to effectively what you can achieve with that kind of chain of custody.
Q. And --
A. And also, I do -- okay. That's fine.
Q. We've already covered paragraph 20 I think pretty thoroughly. I just wanted to ask, on this point, the high risk of attack that you're concerned about for Georgia elections, would you say that Georgia's new election system faces the same level of risk as the DREs, a greater level of risk, or less risk?
A. I think for very important -- for probably the most important category of risk, which is the risk of nation state attacks against close elections, the risk is not substantially reduced. I think for other scenarios, there are some benefits to security from

the change. But sort of the thing that we all should be most worried about, the security of the new system is not -- is not such that those attacks are strongly prevented.

Q. So it's your testimony that Georgia faces basically the same amount of risk from a nation state attacker with its new voting system as it faced with the DRE system; is that right?

A. Unfortunately largely because of the lack of strong auditing and the difficulty of verifying -- of voters actually verifying their ballots well.

Q. If Georgia implemented proper, as you would categorize them, robust auditing procedures, would the security situation from a nation state attacker be improved over the DREs?

A. Well, the problems are both the lack of robust auditing and the lack of -- and the lack of a strongly voter-verified paper record. If both of those things were corrected, then I think the relative risk would be lower than in the DRE system.

Q. And you used a distinction there that I want to hone in on for a minute. You refer to a voter-verified paper record. Can you describe the difference in a voter-verifiable paper record and a voter-verified paper record?

A. Sure. So with the caveat that those terms are often not used precisely in the literature and people for years kind of use them interchangeably but without really addressing the question of whether things that were verifiable would be verified. But a voter-verifiable record is one that in principle the voter could verify. A voter-verified record is one the voter actually has verified and ensured is correct.

Q. And so in recommendations, there has been a lot of terminology thrown around of voter-verifiable paper records. Voters have the option of verifying their records in that situation, which distinguishes it from a DRE where there would be no record; is that correct?

A. From a paperless DRE where there would be no record.

Q. Yes. I'm sorry. Good clarification. When I think of DRE, I've only ever voted on a paperless DRE in Georgia. So thank you for that.

In paragraph 21, you say that there is no doubt that Russia and other adversaries will strike again. On what basis are you saying that there is absolutely no doubt they will strike again? I'm assuming you've not talked to President Putin or Vigo Carpathian or somebody about this, right?

A. No. But I follow very closely the assessments of the intelligence community and DHS and the federal government on these questions. And there's every indication that Russia continues at this very minute to be attempting to interfere in the election.

Q. And election interference we can draw as a distinct concept from vote manipulation. Wouldn't you agree those are distinct concepts? Maybe one includes the other?

A. Yeah, maybe one includes the other.

Q. So election interference could include manipulating votes. But merely interfering could be spreading false messages on social media, visiting websites of county boards, scanning for vulnerabilities in a system. Would that be a fair distinction to draw?

A. I think that's fair.

Q. And so in terms of, you know, no doubt that Russia will strike again, I think we covered earlier we don't have any evidence that Russia manipulated votes in any election in the US, correct?

A. That's right. Even though there were significant gaps in the visibility that would make that evidence available.

Q. Over on the next page, page 7, you indicate that the report found that these foreign agents were

successful in attacking at least one state. Was that one state Georgia?

A. No. Not the state that is referred to in the report.

Q. In the last paragraph you indicate that Georgia was among the states Russia targeted. And as we discussed earlier, targeting doesn't necessarily mean manipulation or compromise, right?

A. No. It's just the first step, but it does -- it does speak to -- towards the intent.

Q. And like the Senate Intelligence Committee, the special counsel never found any votes were actually compromised, right?

A. That's right. But again, there were very serious limitations to the available evidence that would, if the votes were compromised, allow us to reach that conclusion. So the best I think that they could say is well, essentially there's no evidence votes have been compromised.

Q. Is it your personal belief that Russia has compromised votes in elections in the US?

A. I don't know.

Q. In paragraph 22, you talk about some examples. I believe we discussed earlier the Ukrainian presidential election. And Ukrain's vote counting infrastructure that you reference there, that was a

system directly connected to the internet; isn't that right?

A. Yes, it was.

Q. At the end of paragraph 22 you say, other adversarial governments and various things might target future Georgia elections. And sitting here, you don't have any evidence that other adversarial governments absolutely will target Georgia elections, do you?

A. No. But there's no reason to doubt that other governments have something at stake in the outcome of future US elections and have the cybersecurity offensive capabilities that they would need in order to -- in order to do that.

Q. But as we talked about, there's a difference in aiming a gun and pulling the trigger, correct?

A. That's correct.

Q. And so you don't have any evidence they will definitely pull the trigger to attack Georgia elections?

A. No, I can't speak to that.

Q. To paragraph 23. This is another kind of summary opinion piece. It's your opinion that Georgia's new voting technology does not achieve the level of security necessary to withstand an attack by a sophisticated adversary, such as a hostile foreign

government. Isn't that statement true of every states' voting technology?

A. So no, I don't think that it is true of every -- of every states' voting technology, at least not in the same sense, because in states that really do have a hand-marked ballot and are or are intending to audit the paper trail rigorously, the attacks that I'm most concerned about, ones that would actually change the election outcome, would not be likely to succeed.

Q. So in your opinion, the necessary preconditions to have the level of security necessary to withstand an attack by a foreign government are hand-marked paper ballots and robust audits; is that fair to say?

A. Those are two of the most important, and there are other components of resiliency that are important too.

Q. So do you have an estimate on what percentage of jurisdictions currently have sufficiently robust audits and hand-marked paper ballots to withstand that kind of attack?

A. It's just a few percent of jurisdictions unfortunately. There's still a lot of work to do nationally. But there are degrees.

Q. So would it be fair to say then that 90 percent of jurisdictions don't have the level of security

necessary to withstand an attack by a hostile foreign government?

A. I'm not sure about 90 percent, but it is a high percentage.

Q. Higher than 80?

A. Probably.

Q. Okay. Now, you have a lab where you do work related to election technology and cyber vulnerabilities, right?

A. I do.

Q. And do you believe your lab has the level of security necessary to withstand an attack by a sophisticated adversary such as a hostile foreign government?

A. No, absolutely not. We are -- we are definitely not, however, running an election system for any state out of our lab.

Q. You do have technology in your lab that could be used to compromise voting systems that are currently in use, though, right?

A. Yes, we do. We try to take the best steps that we can to prevent that. But unfortunately, the reality is that sophisticated nation states have -- hostile nation states have extremely sophisticated cyber offensive capabilities. And the question is more a question of do they really want to attack us, than

can we withstand the determined attack.
Q. So then in the subparagraphs under 23, you provide some scenarios under which attackers could potentially subvert the election technology. And the first is infiltration of the voter registration database to extract, change, or erase records. Do you see that?
A. Yes.
Q. Do you have any evidence that that has ever happened to the State of Georgia's voter registration database?
A. No, I don't.
Q. And it's true that attackers could infiltrate the voter registration database of any state if they were a sophisticated hostile foreign government, right?
A. That's probably true. Although, Georgia's system has specific technical risks that lead me to believe that the risk is higher in the State of Georgia than in other states.
Q. And how many other states' voter registration databases have you studied for potential risks?
A. How many? That's a good question. A handful of other states. Certainly Michigan in great detail.
Q. And when you say a handful, less than five?
A. Probably less than five in detail.

Q. So you've evaluated five states or less of the voter registration databases. And of those, your conclusion is that Georgia is the most vulnerable of those five?
A. I'm not sure that I've specifically ranked or quantified, but I would say Georgia is significantly more vulnerable than it needs to be.
Q. As compared to those five other states?
A. And as compared to some other states that I've studied. It's certainly more vulnerable that Michigan's.
Q. And what other states have you studied?
A. Where else have I studied? I've looked at the voter registration technology in Pennsylvania and in California to some degree. I would have to go back and check.
Q. Okay. And your analysis of the relative risk level is based on -- what kind of factors are you reviewing when you're evaluating the risk to the voter registration databases?
A. Some of the most important factors are things like the age and brittleness of the software involved, who is maintaining it, and what the results of security assessments have been and whether the problems found in those assessments have been completely mitigated.

Q. And have Michigan, Pennsylvania, California conducted sophisticated threat assessments by cybersecurity vendors of their voter registration databases?
A. Michigan has. I don't know about the other states.
Q. And did those -- for Michigan, did they find any potential vulnerabilities in the database?
A. They did.
Q. And did Michigan then mitigate those and correct those?
A. They did.
Q. And did they correct all of them?
A. To my knowledge, they did, yes. In fact, they replaced the entire software system as a result of those analyses.
Q. What software system does Michigan use today?
A. The Michigan software system is one that is called the -- give me just a second. Changing states. It's called the Qualified Voter File database or QVF.
Q. And is QVF a vendor in this space?
A. No. QVF is custom software for the state.
Q. So Michigan decided to build its own software for voter registration database?
A. That's right.
Q. You indicate that the attacks could cause voters to receive the wrong ballot or be prevented from casting

a regular ballot. Are you familiar with the provisional balloting process?

A. I am.

Q. And if there was an attack like the attack you're describing in 23(a), you'd expect to see an increase in provisional ballots for people who weren't in the registration database, right?

A. That's probably right.

Q. Are you aware if there's been such an increase in Georgia from 2016 to 2018?

A. I don't know.

Q. You indicate that they could also be used to steal information that could be used to impersonate voters. You're aware that Georgia has a photo ID requirement for voting?

A. I am. But that doesn't apply to absentee by mail.

Q. So your reference to voter impersonation here refers to absentee by mail impersonation, not in-person impersonation?

A. Not in-person impersonation.

Q. Which is much more of a tongue twister than I realized it was going to be.

A. That's right. Absentee by mail or to access voter registration records.

Q. The second type of attack that you propose, attackers

could sabotage polling place equipment and prevent them from functioning on election day. Do you have any evidence that any sabotage of polling place equipment that kept it from functioning has happened in Georgia?

A. No. Although, the new equipment has only been in use for a very short period of time.

Q. Do you have any knowledge of the physical security requirements for state election board rules surrounding the new system?

A. I haven't reviewed them in detail.

Q. And I'm assuming you haven't visited any counties to review their inspection of how they're maintaining the election equipment.

A. No. Although, I have -- I'm familiar with reports from others who have visited Georgia counties in the past and have seen some of the physical security mechanisms in place.

Q. And was that before or after the purchase of the new system?

A. That was before the purchase of the new system.

Q. So today you don't know what physical security requirements might be available to mitigate an attack outlined in 23(b); is that right?

A. 23(b) is referring not specifically to attacks that

require physical security compromise, but ones that involve compromise of the software and data running in the system by any means, including by remote cyberattack.

Q. Okay. So it's your testimony that the Dominion system is subject to remote cyberattack that could compromise its functioning?

A. Potentially, yes.

Q. You say at the end of that that the attacker could target such sabotage at jurisdictions that strongly favor a particular candidate and cause a partisan shift. You don't have any evidence that that's ever happened in Georgia, do you?

A. No, I don't. Though, again, the system has only been in use a few weeks.

Q. 23(c), you talk about the manipulation of optical scanners or EMS systems to report fraudulent outcomes. Do you have any evidence that's ever happened in an election in Georgia on the new system or any system?

A. No, I don't. Although, the new system is new. And the old system, I don't think anyone has ever done the kind of analysis of the optical scanners and EMS servers that would be required in order to make a strong statement about whether it had happened.

Q. You reviewed the GEMS databases for the state's old system, though, correct?
A. Yes, I have.
Q. Have you discovered any malware compromise in that review?
A. No. But the GEMS databases themselves are no substitute for reviewing the actual software running and installed on the servers.
Q. But you don't know if anybody has undertaken that kind of review in the last six months, say?
A. No, I don't think so.
Q. You indicate that at 23(c), attack could alter all digital records of the election results. And that's where, again, you're coming back to the rigorous manual audit or a recount of the paper ballots. Then you say, Georgia law doesn't currently require that. What is your understanding of what Georgia law does require?
A. So my understanding of what Georgia law requires is that it requires an audit this year but not a risk limiting one. It requires an audit pilot by the end of 2021. And that after that, the requirement depends on the outcome of the pilot.
Q. And you don't know what Georgia's current plans are related to auditing of ballots going forward on the

new system, correct?
A. Auditing ballots on the new system. My understanding is that Georgia does not require -- does not currently plan to require a rigorous audit.
Q. Have you reviewed any state election board rules related to audits in Georgia?
A. I have reviewed some state board election rules related to audits in Georgia, but I can't -- I'm not prepared to tell you exactly what the -- which set of rules those were. I just don't remember.
Q. Are you aware that Georgia is working with Verified Voting on the development of its audit processes?
A. I'm aware that they were -- that they have been working together in the past.
Q. And do you support that kind of collaborative effort to develop audits for jurisdictions?
A. Well, look, I support work to implement robust audits, but you have to actually get there in order to have the benefit.
Q. Do you based on your expertise in the design of audits believe that piloting audits is a helpful practice before you implement a full audit procedure in a jurisdiction?
A. Yes, I do. But you have to actually implement the full audit procedure in the jurisdiction.

Q. And the type of attack you outline in 23(c) is also true of a hand-marked paper ballot system; is that correct?
A. Yes, that's correct.
Q. In 23(d) you talk about an infiltration to sometimes print ballots differing from a voter's onscreen selections. And it's basically (d) and (e), the way I read them, are two types of attack, one that changes only the bar code, one that changes the bar code and the human readable text. Again, you indicate that a 23(d) attack must be rigorously audited or else it could go undetected. Is that a fair statement?
A. That's right.
Q. And so it's your testimony that a sufficient audit would mitigate against the 23(d) style of attack, right?
A. That's right. But it would have to be an audit that was more rigorous than any audit that I understand to be planned in Georgia.
Q. But you don't currently know what's being planned in Georgia; is that right?
A. Well, I know what's being -- what's been publicly talked about in Georgia, and I told you what my understanding of the legal requirement is.

Q. Have you ever seen a, and this is going to be in any context, lab or otherwise, a virus or malware that would alter only the ballot bar code on a Dominion system?
A. On a Dominion system, no, I have not.
Q. Have you ever seen in the lab or otherwise a piece of malware or virus that would alter both the bar code and the human readable text on a Dominion system?
A. No. Although, on other systems I have.
Q. In 23(e) when you say research shows that few voters carefully review their printed ballots, you're referring to the two studies you cite later in your report; is that right?
A. Yes, I am.
Q. And no other studies beyond those?
A. I'm referring to those two studies.
Q. And you say that the fraud sufficient to change the winner of a close race might go undetected. One thing I've always wondered about these kind of possible scenarios is how would an attacker know what will be a close race?
A. Right. So usually by pre-election polling is one way that an attacker can potentially conclude that a race is likely to be close.
Q. And in races where there's not regular polling, for

example, smaller races, are there other methods someone could try to use to determine what they would need to alter?

A. I'm sorry. Can I actually turn this off?

Q. Sure.

(Recess taken.)

THE WITNESS: I'm sorry. Can you repeat your question, please.

BY MR. TYSON:

Q. Sure. So in a race that is a smaller jurisdiction where there's not regular polling, for example, of a race, state house race, county commission race, how would an attacker go about determining what would be a close race that they could try to throw in that context?

A. Well, they could cheat anyway just in case it's close, right? So they don't necessarily need to know for sure that it's going to be close in order to attempt an attack and succeed if it is, in fact, close.

Q. And then in 23(e) you indicate that no audit or recount could detect that kind of attack because the digital and paper records would be wrong. And the only way -- now this is me. Is it correct that the only way a 23(e) attack would be detected is if a

sufficient number of voters carefully reviewed their printed ballots?

A. That's the only surefire way that such an attack would be detected, and then also assuming that there was a careful audit of the paper trail.

Q. So the way I read this, the attacks you outline in (c), (d), and (e) could be mitigated or detected by sufficiently rigorous audits with voters carefully reviewing their printed ballots in a sufficient number. Is that fair to say?

A. I think that's fair to say.

Q. And the attack outlined in (a) would be mitigated by the use of provisional ballots, right, and possibly detected through a spike in provisional ballots there?

A. Well, all right, wait a minute because it's -- it matters a lot what we mean by mitigated. That attack in (a) would at least be detected as a result of a spike in ballots. But if it's already caused there to be long lines or other chaos at the polling place, there's no way that you can go back and fix it.

Q. Okay.

A. These other attacks in I think you said (c), (d), and (e) were mitigated by a combination of voters robustly verifying -- or rigorously verifying their

ballots and a sufficiently robust audit. Although that's true, I don't think that there is any -- that there is sufficient evidence to conclude that it's possible to induce voters to rigorously verify their ballots to the necessary level in an all BMD context.

Q. And you made an important distinction. So there are methods by which (a), (c), (d), and (e) can be detected, and then there will be at least some basis to go and investigate further what actually happened. Is that fair to say?

A. So we have to -- we should probably make a diagram about that or something like that to distinguish exactly which circumstance detection versus correction is possible.

Q. Why don't we try it this way? Under (a), you can detect an attack outlined in 23(a) by a spike in the provisional ballots for individuals not in the voter registration database.

A. Depending on which variation of this attack. But for plausible variations, I would agree with you.

Q. And then for (b), I'm assuming that would be relatively obvious because things are not working. So that would be a very detectable type of attack?

A. Yes. Hard to recover from, but one that you know chaos is happening.

Q. And (c) can be detected through a sufficiently robust audit or a recount, correct?
A. Yes.
Q. And (d) can be detected through a sufficiently rigorous audit.
A. Yes.
Q. And then (e) can be detected --
A. Although, (d) cannot necessarily be corrected by a sufficiently rigorous audit.
Q. That's why I'm asking specifically just the detection question for each of these.
A. Yes. Okay.
Q. And then for (e), it can be detected through sufficient number of voters carefully reviewing their printed ballot and sufficiently rigorous audits.
A. Yes.
Q. Okay. And in each of those scenarios, there would then be a basis to conduct a further investigation to find evidence of the types of attacks that have been outlined, right?
A. Well, it depends. So in some of those scenarios, it's too late. The election has already been disrupted. In other cases, in other cases, if you detect that something is wrong, you don't have any information available by which to go back and correct

the changes that have happened.
Q. You're familiar, I'm assuming, with the process of an election contest?
A. Yes.
Q. And so there already exists provisions in Georgia law and I'm sure other states as well that if, for example, people who were ineligible incorrectly vote, there's a provision to handle that through an election contest. Are you aware of that?
A. Yes.
Q. And so you said it's too late in terms of, you know, once we detect it. But if we detect it and an election contest is filed, the election can be re-run, just like it would be if ineligible people were voting, right?
A. That's true. I would hate it -- I would hate to be Georgia if we have to re-run the 2020 presidential election because of Georgia's voting system.
Q. And it's your testimony that you don't have any evidence that any of the attacks in (a) through (e) have ever occurred in an actual election in the United States, right?
A. No. But election systems in many jurisdictions in the United States don't produce the kind of evidence that we'd need in order to know that these attacks

have happened.
Q. In paragraph 24, you begin discussing malware, malicious software that could be introduced into the election equipment. You don't have any evidence that malware has been introduced into election equipment in use in elections in Georgia, do you?
A. No, I don't. Although, to my knowledge, no one has done the kind of forensics to any piece of election equipment in Georgia that would be the most probable way to detect such malware intrusion if it occurred.
Q. And the list of introduction of methods of malware introduction in 24, that's true in every state, correct? You could introduce malware if you had these types of things into optical scanners, for example, in every state system or election management system?
A. Yes. That is true.
Q. In paragraph 25, you begin with a little bit more detailed discussion of the pieces connected to the internet.
A. Could we maybe take a break at some point soon?
Q. Certainly. I'm fine to take a break now, if you'd like to.
A. All right. If we could.
Q. Absolutely. Thank you.

(Recess taken.)

BY MR. TYSON:

Q. So turning to paragraph 25, we talk about some components oven the system that are directly connected to the internet.

A. That's right.

Q. Now, we've discussed a little bit the MVP and OVR systems. What is your understanding of how the MVP system is connected to the eNet database?

A. Well, let me see if I can remember for this specifically for the MVP. The MVP -- the MVP I know receives information from the eNet database and I believe contains a way to update that information. But that may be in the OVR system. It's been a while since I've looked at them independently.

Q. And so the OVR system, do you understand how that is connected with the election system?

A. Well, it generates voter registration requests that I understand have to be reviewed by a person, but that data then is fed into the database.

Q. And are you recommending that no voter registration information be put online for security purposes?

A. No. But what I'm recommending is that especially heightened security precautions should be taken for the components that are online because they create a

path by which an attacker could potentially come from anywhere in the world and access the system.

Q. In the third sentence of paragraph 25, though, the criticism seems to be just that they are connected to the internet.

A. This isn't a criticism. This is an expression of -- an expression of the nature of the risk.

Q. And so this is a risk that there's at least a good policy reason to encounter because we want voters to have information about their voting information?

A. Perhaps. And it's a risk that -- but it's also a risk that is especially heightened in Georgia due to the nature of the problems that have already been detected in the eNet system and the reviews that have happened so far.

Q. You don't have any evidence that Georgia's eNet system has been directly targeted by malicious actors, do you?

A. Just the broad conclusion of the Mueller investigation and the Senate Intelligence Committee that Georgia was among the states whose systems were targeted by Russia in 2016. And I think it's a inference that the online components of the registration system were among those targeted.

Q. Do you know how Georgia maintains backups of its eNet

registration system or if it does?
A. I believe it does, but I don't know the specifics about how those backups are maintained. And it's a good thing that it does.
Q. In paragraph 26, you talk about components that are not connected to the internet that could be targeted. And one of the ways is removable media. And you cite the Stuxnet computer virus. Are you with me on that?
A. Yes.
Q. And it's your testimony that that was attacked through removable media and not through programming at the manufacturer?
A. Stuxnet was designed to, among other things, spread through removable media.
Q. Did the initial infection of Stuxnet come through removable media?
A. I think I've seen conflicting reports and conclusions about that, but the way that the Stuxnet malware was designed was able to spread to disconnected systems by a removable media.
Q. And in the next sentence you say that attackers could employ this method to infect state or county EMS and spread from there to scanners and BMDs when workers program them for the next election. Do you have any evidence that this has ever happened to a Dominion

system?
A. No, I do not. Although, the Dominion system is very new.
Q. So let's talk about the Dominion system. That leads up to paragraph 27. And your opinions in this section about the Dominion components, I think we've discussed, came from your review of the technical documentation, the California and other evaluations of it, not from your personal review, correct?
A. That's correct. They're based on my experience with other similarly designed voting systems as well.
Q. Now, you in paragraph 27 say, Dominion does not dispute that its devices can be hacked by sufficiently sophisticated adversaries. And that's not really that remarkable of a statement, is it? I mean, can't any computer, we've already discussed, be hacked by sufficiently sophisticated adversaries?
A. I think that's actually a critically important point because this is the entire reason that we need the paper trail, the paper trail to reflect accurately voters' intentions and the paper trail to be rigorously audited.
Q. So you would agree that that's not really a remarkable statement, though, because it's a computer that can be hacked, which is basically every

computer?
A. I agree that it's basically every computer that can be attacked. But again, that's really a core part of why Georgia even has a new voting system right now, that all computer systems can be hacked, and we need to be very, very careful to make sure that, you know, voting system context, the correct outcome is going to be determined even if the systems are successfully attacked.
Q. The first reason you cite, you say one reason why this is true. So you're going to give, I guess, a couple of reasons why it can be hacked. I guess isn't the first reason why it's true is because it's a computer?
A. I suppose so.
Q. Okay. You first cite the complexity of the software, though. Have you compared Dominion's software with the number of source code lines in other BMD systems?
A. In other voting systems. Not -- I'm not sure it's specifically in other BMD systems.
Q. And is it your testimony that the number of lines of code is higher in the Dominion system than other voting systems?
A. It's ten times as much code as Georgia's previous voting system.

Q. And compared to other ballot marking device systems?
A. I don't know. It's probably similar, but I can't -- I can't estimate exactly how much. Probably -- yeah. I can't estimate how much.
Q. The ICP scanner you indicate has 475,000 lines of source code. The ICP scanner is the optical scanner, right?
A. The precinct-based optical scanner as opposed to the central count.
Q. And is that similar to the number of lines of code for other precinct-based scanners you've evaluated?
A. It's more code than for other precinct-based scanners that I've evaluated by something like a factor of three or four.
Q. And you indicate that the software is written in C/C++, and you say that that programming language is particularly susceptible. Is that true of all software written in C/C++, that it's more vulnerable than other software?
A. It's extremely difficult to write software in C and C++ that is even reasonably secure to the point that I'm advocating that my department stop teaching those programming languages to undergrads.
Q. Are those programing languages used in commercial applications today?

A. They are. Although, decreasingly so because of the security risks.
Q. And the security risks on the C, C++ front on the precinct scanner are there for hand-marked paper ballot systems too, correct?
A. Yes. That's part of the reason that the system needs to be audited.
Q. You say in paragraph 29 that software the size and complexity of Dominion code inevitably has exploitable vulnerabilities. So is it true then that just having a large number of lines of code always leads to exploitable vulnerabilities?
A. In practice, yes.
Q. The quote at the end of 29 from the California study, if the system were secure, it would be the first computing system of this complexity that is fully secure. Would you ever categorize any computing system as fully secure?
A. There are some simple computer systems for which you could plausibly make such a statement, but they're very simple computing systems.
Q. Like an Atari-level computing system?
A. Probably not even that.
Q. And so when you reference nation state attackers in 29 discovering and exploiting novel vulnerabilities

in complex software, that basically is pretty much every piece of software has exploitable vulnerabilities, right?

A. That's right. It's another way of saying that if the Russian government decides to target Georgia's elections in 2020, they're likely to succeed.

Q. And ultimately, that's not a function of a Dominion system, a function of the lines of code. It's just a function of it being a computer that's programmed by software, isn't it?

A. And a function of the lack of things like a strongly -- a paper trail that voters -- a paper trail that we can be sure reflects voter intent even in the face of attack and a question of whether there is a rigorous enough audit.

Q. And so essentially it's your testimony that there is no way we can ever secure any computerized voting system adequately, which is why you advocate for a hand-marked system primarily?

A. I'm not opposed to the use of technology in voting in general, but that technology has to be used in ways where we don't have to trust that the technology is functioning correctly in order to be sure the election outcome is right.

Q. But you would never place a piece of technology

between a nondisabled voter and the ballot?
A. I think it's unwise to do that if there were alternatives, and hand-marked paper ballots are such an alternative.
Q. In paragraph 30, you talk about using outdated off-the-shelf software modules. Isn't that a relatively common practice when designing software?
A. It's actually not a common practice among well-written software. Well-written software today tends to use automated methods to make sure that the dependencies are up to date.
Q. And so when we discussed earlier the use of open-source software and off-the-shelf hardware, you're saying it's not a good idea to use off-the-shelf software; is that fair?
A. I'm saying if you're going to use off-the-shelf software, you have to make sure that it's up to date every time that you're shipping a new version of your product and you have to ship a new version of your product every time there's security updates to those downstream dependencies. That's a critical part of the modern software development, of modern software development practices that isn't reflected in the Dominion system.
Q. And every EAC-certified system has to have its

software certified and maintained by the EAC; is that correct?

A. Tautologically every EAC-certified system has to have its software certified. That's right.

Q. And the certification process includes the EAC maintaining a gold disc of that version of the software that is the certified version; is that correct?

A. That -- essentially, yes.

Q. And so any time a software manufacturer wishes to make any change, including a security update, they'd have to get their software recertified by the EAC, right?

A. That's part of the problem with the Georgia voting system, that, in fact, its software is out of date because a new version -- if there were security updates needed, they're likely going to have to go through further certification before they can be used.

Q. So that's a yes, it has to be recertified if there's changes for security?

A. It depends on quite what the changes are. But sometimes it has to go through a complete recertification.

Q. In paragraph 31 you say, outdated software components

are a security risk because they have these documented vulnerabilities, and you cite, for example, a list of 254 known vulnerabilities. Is a vulnerability always an exploitable vulnerability? How are you using the term vulnerability in this paragraph?

A. Whether it's exploitable or not in this context depends on what the -- depends on the specifics of the particular problem and what the attacker is trying to do.

Q. So the fact that an Android operating system has 254 known vulnerabilities is just like saying it's a piece of software, right, because every software has vulnerabilities?

A. Well, no, not exactly. The problem is that it's a much stronger statement than simply it's a piece of software. This is a piece of software that's already been analyzed, people understand where many of the vulnerabilities are, and I can provide a recipe to make it even easier for an attacker to get in or to allow less sophisticated attackers to successfully compromise the system that don't have the resources of a nation state.

Q. So the fact that there are 254, does that tell you anything about the relative risks of the use of this

particular version of Android?
A. As compared to --
Q. In the election contest, I should say.
A. As compared to newer versions of Android?
Q. As compared to anything. Does the fact of the number of known vulnerabilities tell you how vulnerable a piece of software actually is?
A. It's a good indicator. It's certainly an indicator of the level of vulnerability. And 254 unpatched vulnerabilities is a very bad situation to be in.
Q. And is that number higher or lower than the number of known vulnerabilities in other BMD systems?
A. I don't know the number of known vulnerabilities in other specific BMD systems off the top of my head, but I can tell you that in absolute terms that's pretty high.
Q. Your next paragraph, 32, talks about a cheap security officer position that was vacant. How is this paragraph 32 informing your analysis of the relative risk faced by Georgia? And the reason why I ask that is, from our discussions so far, it sounds like it's a piece of software, it's a computer, it's going to be vulnerable. How is the existence or not of a chief security officer informing your analysis?
A. Well, this is informing whether Dominion is following

best practices in its security and its software development and maintenance. And not having a chief security officer in place, I think is a sign of a general -- is a sign of a general perhaps difficulty in achieving security best practice.

Q. So are you opining that Dominion does not take security seriously?

A. That the position is still vacant does not speak highly of Dominion's security posture. I'm opining that there is -- that this is -- that this is a sign of lax security practice.

Q. And it's your testimony that the Dominion software is not secure software, right?

A. Yes.

Q. And it's also your testimony that every ballot marking device software is not secure software, right?

A. It is my testimony that no ballot marking device is likely to be able to withstand a sophisticated nation state attack, and that's why it's so important that we have -- that all jurisdictions practice -- that all jurisdictions -- that's why it's so important that ballot marking devices be -- that the scope of use of ballot marking devices be limited.

Q. And you haven't done a full comparison of every

ballot marking device that's currently available, right?

A. That's right.

Q. And you haven't asked Dominion who has responsibility for security development and implementation of security in Georgia?

A. No, I haven't. It's unclear who, if anyone.

Q. In paragraph 33 you say, Georgia certified the system without performing its own security testing or source code review. The system Georgia used is certified by the EAC, right?

A. Yes. So were versions of Georgia's old system.

Q. And part of the EAC's review for certification involves security, correct?

A. A very limited kind of security testing unfortunately. It's not rigorous.

Q. So it's your testimony a state can never rely on EAC certification for cybersecurity issues?

A. I think it would be very foolish to rely only on the EAC certification for security. That's right.

Q. In beginning of paragraph 34 we begin a walk through the California test, which is a different version than the version used in Georgia, right?

A. It's a more recent version.

Q. And I believe we've already covered this. But you

weren't involved in any of the California review of the Dominion system, right?
A. No, I was not.
Q. You say in paragraph 35 that, like all security testing, California's tests were necessarily limited and could not be expected to find all exploitable vulnerabilities. Can you tell me about what you mean by that sentence?
A. Right. So security testing -- security testing can expose the existence of vulnerabilities. It can't in general prove that systems have no vulnerabilities.
Q. So you can't prove a negative basically. I can't prove there are no vulnerabilities?
A. Not with the normal means of security testing.
Q. And is that why the security testing is necessarily limited in scope, because it's just not possible to find everything?
A. Well, in part. And there's also a question of the rigor involved. For instance, the California top-to-bottom review of the -- in 2007 of the equipment that Georgia has just gotten rid of spent something like a man year of effort per system doing code review, right, a very high level, an intensive level of review. Security testing of the kind I understand that California does now, it's a much more

limited time and scale. There's a quantifiable -- there's sort of a quantifiable difference as well.

Q. So ultimately it's a policy decision how much effort a state wants to put into its security testing. Is that fair to say? California chose at one point to do a massive amount of it. Now it chooses to do something less.

A. I suppose you could characterize that as a policy decision.

Q. Would you characterize it as something different?

A. No. Again, I suppose you could characterize it as a policy distinction. I'm not sure I would characterize it differently.

Q. So in paragraph 35 you kind of distinguish the two versions to say more recent versions of software tend to contain fewer security vulnerabilities. But you haven't done any comparison, and to your knowledge no one has, to know if that's the case, right, if there's more or less vulnerabilities?

A. Right. Unfortunately, Georgia didn't do its own security testing of a similar kind to California. So we don't have a direct comparison.

Q. And you haven't -- I'm sorry.

A. But in general, it's true that as software evolves, vulnerabilities are corrected at a higher rate than

they're introduced.
Q. And you have not done any security assessment of vulnerabilities in Georgia's Dominion system, right?
A. No. I haven't had the access to do that.
Q. The next paragraph talks about the installation -- software installation files and a belief that it was possible to inject things into the system. And you say, this implies that attackers could modify Dominion installation files. But I'm assuming you've never tried to do that, right?
A. No. I have not had the access to try to do that myself. This is based on what California's testers found.
Q. And California's testers, again, looked at the antivirus available. Do you know if that same antivirus is used in Georgia's system, or not?
A. Yes, it is.
Q. And you reference that the ballot marking device and the precinct optical scanners have no antivirus software at all. Would you expect to find antivirus software on a precinct scanner?
A. Some precinct scanners can have antivirus software. It depends -- it depends on the specific scanner.
Q. And so are there particular manufacturers that install antivirus software on precinct scanners?

A. Yes. So let me see. No. I can't -- I can't recall off the top of my head. But yes.
Q. And so then the end of paragraph 37 you're saying, malware that infected the Dominion components could evade antivirus protection. Again, that's possible, but you don't know for sure, right?
A. Well, with California's -- what California's test found was, in fact, they tried to see if the antivirus would detect malware samples, and in some cases it failed to do that. So that's the basis for that conclusion.
Q. And that was just specifically for the EMS server and not for -- California didn't run those tests on the BMD or the optical scanners, right?
A. Well, the BMDs and optical scanners don't have antiviruses. So tautologically malware could evade antivirus detection in those components.
Q. And are you aware whether Georgia requires any other components on the EMS server that would address malware antivirus software different than California?
A. I'm not. But it would invalidate the EAC certification for them to install such components.
Q. So the EAC certification extends to the antivirus components of the EMS server?
A. Yes.

Q. Paragraph 38 there's a discussion of physical access to a USB port. And you say, this implies that no secret passwords or keys would be needed to exploit the problem, given physical access. Isn't that a huge given under the circumstances that you don't know what physical access requirements exist for Georgia BMDs?

A. It's very difficult to have a physical access regime that would prevent any physical access under any circumstances by an attacker. So I think it's quite significant that someone with physical access could potentially alter the software running on these devices.

Q. If I gave you an unencrypted computer, physical access to an unencrypted computer, no matter what security measures I had on there, you could hack that computer, right?

A. Oh, definitely.

Q. So doesn't physical access matter a lot then, the protocols around physical access?

A. The protocols around physical access are important. But there's the question of, for instance, is the computer actually encrypted. If it is encrypted, it's going to be more difficult to do something hopefully for someone with physical access.

Q. But ultimately since you were not aware of Georgia's physical access and physical security requirements, the statement in paragraph 38 doesn't really add much to your analysis because we don't know what type of physical access or what would be involved in someone gaining physical access in Georgia, right?

A. I'm not sure that I would agree with that. I think whatever the level of physical access protection that Georgia has, the fact that given physical access without any kind of secret information someone could exploit the problem that the California reviewers found creates significantly greater risks than if the system had been designed without that problem.

Q. So you say at the end of 39, these problems indicate that the Dominion system was designed without sufficient attention to security. And so that's, I guess, consistent with what you said previously. You don't believe there was any attention given to secure -- sufficient attention given to security. But ultimately, isn't it true that you find these kind of vulnerabilities or problems with every computer? I guess what I'm trying to understand is, you're opining about Georgia's Dominion system, but really you're opining about ballot marking devices generally. I'm at a loss to see if you can never

sufficiently secure these systems, why is Dominion's system any different than any other ballot marking device being used today?

A. So there are things that are true about all software and all ballot marking devices, and there's further evidence that these things are true about Georgia's system specifically. And, in fact, some of this is what California's finding helps to suggest even more specific recipes by which an attacker could strike the Georgia Dominion system. And this all gets back to, once again, why the lack of sufficiently robust audits and the universal use of BMDs for in-person voters lead to such significantly heightened risks.

Q. And that's true whether it's a Dominion system or any other system if you're using BMDs for all voters, right?

A. Many of the same problems would in here.

Q. And going to paragraph 40, ultimately California chose to certify the Dominion system, right?

A. They did.

Q. And you know that they imposed much more stringent security conditions than those in Georgia. How do you know that Georgia didn't adopt or utilize any of the security conditions that California recommended?

A. Based on -- based on my knowledge to date about what

procedures, publically available procedures Georgia has promulgated.

Q. So the statement that California imposed certification or more stringent security conditions than those in Georgia is based on the Dominion documentation you reviewed?

A. Yes, in part. In part on the California documentation I reviewed, and in part on the overall security posture of the Dominion system as used in Georgia.

Q. And you disagree with California's decision to certify the Dominion system, right?

A. In part.

Q. What do you mean in part?

A. In part. I think the -- so the -- California, because it has more stringent auditing requirements than Georgia, faces somewhat less risk. And California does not -- most California jurisdictions don't use the BMDs for all voters. And in those cases, they don't suffer from the same risks from BMD-based attacks. So I think the risk is less in California than in Georgia. I still think that there's a risk in some California jurisdictions if they're going to use BMDs for all voters. But I think the way that the system is used in most of

California is less risky than Georgia.
Q. Is it your opinion that a California county that uses BMDs for all voters with these more stringent security conditions has an acceptable level of risk?
A. No.
Q. So ultimately, even if Georgia agreed to every security condition in California and imposed that for all its BMDs, the fact that it's using BMDs for all voters would be the thing that would -- that you would say that's the security risk; is that right?
A. Yes. I think the BMDs for all voters, coupled -- they would need both the BMDs -- they would need both sufficiently rigorous audits and not -- and to be using BMDs for only a smaller fraction of voters in order for the Dominion system with any set of security precautions to be adequately safe.
Q. So there is no situation where BMDs are used for all voters, based on your current understanding of the landscape, that you would say that was an appropriate level of risk in an election system. Is that right?
A. I think that's probably safe to say. Though, there are matters of degree within that level of risk.
Q. Which gets back to, I guess, our earlier discussion about acceptable levels of risk. Sitting here, do you have a way by which you would determine the

acceptable level of risk for a BMD-for-all system?
A. Yes. So in part, this is based on empirical observations about voters' likelihood of catching errors as in our January study, right? And you can use that to estimate for a given BMD deployment and what fraction of voters are using it what -- how much evidence you would have of systemic error for a particular closeness of an election result. That's one way of evaluating in a very quantifiable way the relative risk.
Q. And I apologize if I'm just not grasping the concept. This is probably me, not you, so don't take this the wrong way.
A. It's probably me.
Q. I just am trying to understand. Ballot marking devices for all voters is a scenario that you say imposes a high risk such that it's too much risk. You can point to the voters verifying at a level. And so is it that if voters verified 90 percent of their ballots, you would then say that's an acceptable degree of risk for a BMD-for-all system?
A. So the analysis is basically of the form, given this fraction of voters using the system, is there -- is it -- is it at all likely that election officials are going to notice systematic fraud sufficient to change

the outcome of a close election if attackers are able to compromise the machines. And if the answer is yes, it's very likely, then that's probably an acceptable risk. If the answer is no, it's quite unlikely, then that's an unacceptable risk. So there's some gray area in between, but we're not in that gray area with Georgia's machines.

Q. And when you say we're not in that gray area with Georgia's machines, I know we're not for the voter certification. Are you saying the security vulnerabilities alone take us out of the voter verification question?

A. No. The overall posture of deployment takes us out of the -- out of the gray area there. That they are used by all -- that they are used by all voters unfortunately takes us out of that gray area.

Q. So it is correct then that if BMDs are used for all, we're out of the range of acceptable risk under any construct?

A. At least for BMDs that are available today. It's possible that future BMDs, some very different design might result in different verifiability properties, that voters would have a much easier time verifying them. Or perhaps someone will discover eventually a way to get voters to reliably verify everything on

the ballot, but it seems extremely unlikely to me at this point.

Q. So let's move to voter registration database. And you talk about a cyber risk assessment of eNet from two years ago. Is that correct?

A. That's right.

Q. And I'm assuming you are relying on the publically available information from the Curling case for paragraph 41 and 42.

A. Yes.

Q. Okay. You say that the PCC assessment or the assessment of PCC software was limited in scope. But didn't we just say in 35 that all security testing is limited in scope?

A. This was particularly limited in scope.

Q. Okay. So too limited?

A. It was particularly limited in scope. The 2018 assessment, if I'm recalling correctly, was basically just a functional assessment and didn't even get into the inner workings of the code.

Q. And you've not personally examined Georgia's security environment for eNet or the software that Georgia -- or the eNet software itself in Georgia, correct?

A. No. Although, I'm familiar with the risk assessments that Georgia commissioned in that environment.

Q. In paragraph 42, you state that transferring the operations does not mitigate the full range of issues, and then you say the state has -- there's no evidence the state has taken other steps to address them. What is your basis for that knowledge today? This is -- you know, we're what, eight months past the hearing where these issues were discussed. Is it your understanding that Georgia still has not mitigated these?

A. I'm aware of a -- I'm aware today of a very recent status update in the Curling case where Georgia asserts that it has taken some steps. Although, I'll note that update is devoid of sufficient technical detail to have -- to conclude that the progress is substantial. It just says that some things have been mitigated and others are still in process, which based on previous testimony in the Curling case about vulnerabilities that would have led someone to believe that vulnerabilities were corrected in these systems when they had not been corrected, I think leaves me with significant reason for doubt.

Q. You don't know sitting here today whether Georgia has contracted with any cybersecurity vendor for any of the more detailed security assessments that you recommend, right?

A. I'm not sure.
Q. And you don't know if Georgia's review of its mitigation steps for the security assessment that were outlined has been reviewed by its outside cybersecurity vendors, do you?
A. No, I don't.
Q. And if all of those -- the full range of issues had been fully mitigated, as recommended by the cybersecurity vendor, would you have greater confidence in the secure of Georgia's voter registration database?
A. I think it would also require further assessment and source code review and mitigation of the things found as a result of that before I would say I had further confidence. And the level of further confidence would depend on the details of those analyses.
Q. And those types of analyses cost money, don't they?
A. Yes, they do.
Q. In paragraph 43 you talk about attempts to infiltrate the voter registration system. And we've discussed -- I think we discussed that piece already about the internet connection. But you say serious vulnerabilities in the MVP website were discovered on the eve of the November 2018 election. What were those serious vulnerabilities?

A. Yes. So there were vulnerabilities in the websites that would have allowed an attacker to access the voter registration data of many individuals without their cooperation or knowledge and that would have allowed an attacker to access system files on the server that were not intended to be exposed, potentially critical components of the inner working of the services.

Q. Georgia's voter registration information about identifying information on voters is public record, isn't it?

A. I don't believe that everything in the file is a public record.

Q. And you say in the next sentence, unauthorized parties could have exploited these vulnerabilities to access sensitive system configuration files and voter registration data. What's the basis for the statement that they could have accessed -- I'm sorry. I meant to ask about the next sentence.

This information would have allowed attackers to fraudulently change voter registrations through the OVR system. What is the basis for that statement?

A. That the information contained in the My Voter Page was sufficient to authenticate as a voter to the --

to the service that allows you to update your voter information, like where you live. And so it would be possible for an attacker to use that information to change the records of voters and cause them to be registered in the wrong jurisdiction, for instance.

Q. Is it your testimony that this type of attack could have immediately updated the eNet system without going through a registrar?

A. No. Although, I'm not sure that there is evidence either that registrars would have spotted this attack had it taken place.

Q. And there's no evidence that this type of attack occurred and that any registrations were ever changed, correct?

A. That's correct. But I think it speaks to the level of security preparedness of the voter registration system.

Q. Is it your understanding that the voter registration system is at issue in this case?

A. These are components of the voter registration system by the definition used in basically every state.

Q. And my question was, is it your understanding that the voter registration system is at issue in the Fair Fight Action case?

A. Yes, I do understand that it is at issue.

Q. Next we move to the electronic poll books in paragraph 44. And we covered you have not personally reviewed the Poll Pad e-poll book, correct?
A. That's correct. I'm relying on the information provided by Dominion, which included technical documentation for the Poll Pad and on the analyses done in other states and my expertise.
Q. Are you aware whether Georgia requires the wireless and internet capabilities of Poll Pads to be disabled?
A. I understand that it requires that during the process of voting while polls are open, but that's -- that the WiFi be disabled. But I don't believe that it requires that to be disabled at other points.
Q. Do you know if Georgia has taken any steps to permanently disable that access on Poll Pads?
A. I don't know.
Q. In paragraph 45, you discuss an attack to alter voter registration data in the Poll Pads. Are you aware that Georgia requires paper records of all registered voters in a precinct at each precinct?
A. Yes, I suppose I do know that.
Q. So if an attacker altered voter registration data or disabled the Poll Pads, Georgia election officials would have a way for voting to continue, correct?

A. To continue, although possibly at a much slower rate, which could cause chaos on the ground.
Q. But you haven't assessed what the rate of check-in would be with a paper list versus an electronic list?
A. I haven't. But it's fairly easy to -- I think it's a reasonable conclusion that it would be slower without the use of the technology.
Q. And so ultimately it was a policy decision Georgia made to include technology for this purpose possibly to speed up the check-in process?
A. Or to decrease the cost of the check-in process.
Q. You say in paragraph 46 that Georgia -- to your knowledge, Georgia has not performed any security testing of the Poll Pads. It's possible they performed that and you don't know, right?
A. I suppose it's possible that they performed their own testing and didn't tell anyone about it. But that would seem -- but I've been following the case with the Georgia system carefully, and to my knowledge, they have not.
Q. Do you know if Georgia relied on the California review when it made the selection or decided to go with the Poll Pads?
A. I don't know.
Q. And in 47 you indicate that California conditionally

certified the Poll Pads subject to 19 terms and limitations. Do you know if Georgia adopted any of those terms and limitations?

A. I don't know. But one of the most important ones was that the Poll Pad not be used to program or encode smart cards that would interface with the BMDs, and it's my understanding that Georgia has not adopted that one.

Q. And Pennsylvania also conditionally certified the Poll Pad, right?

A. That's right.

Q. And they had some additional conditions and security recommendations. And you don't know if Georgia has adopted those at any point in its implementation of the Poll Pad, right?

A. I don't -- I don't know. Although, again, one of the most important ones in Pennsylvania was the prohibition on encoding smart cards from the Poll Pad because that creates a path from the Poll Pad system to the BMDs. And Georgia does encode voter access cards from the Poll Pad is my understanding.

Q. If Georgia adopted all of the terms, limitations, and security recommendations imposed by California and Pennsylvania, would you still recommend against the use of the Poll Pad?

A. It would certainly further reduce the risk.
Q. Would it reduce it to an acceptable level?
A. Perhaps. It's subject to -- subject to other security conditions as well. So that alone would not necessarily be enough.
Q. So when you say subject to other security conditions, what other security conditions would it be subject to?
A. Well, I think it would take some time to do a full analysis of that question.
Q. And what process are you using to determine the relative level of risk of the Poll Pads with and without the California and Pennsylvania conditions, or are you using one?
A. So this is -- to determine the relative risk in that case, this is what would -- what I'm doing to determine that is modeling the different paths by which an attacker might attempt to spread infiltration through the voting system. And so one of the critical differences between the Georgia and California and Pennsylvania models of using the Poll Pad is the existence or not of this path from the Poll Pads to the ballot marking devices.
Q. In my hypothetical I asked you to assume that we adopted all the Pennsylvania and California

conditions, which would include the prohibition on that path.

A. That's right.

Q. How would you evaluate the level of acceptable risk given the adoption of all those conditions?

A. Well, I think it would involve a security analysis of what the remaining modes of infiltration were and what the -- what the full set of protection measures allowed for or required in terms of a fail-safe.

Q. And you haven't conducted that kind of analysis here, right?

A. Not in your hypothetical, no.

Q. And you haven't conducted it as part of your report, correct?

A. I don't really need to in terms of this report because the significant risk of the infection spreading from Poll Pads to the BMD systems is itself -- is itself the focus of my analysis here.

Q. So the fact that items are being taken from the Poll Pad to the BMD is a sufficient basis to determine that is an unacceptable level of risk to encounter in an election system, correct?

A. That was sufficient to convince California and Pennsylvania to prohibit that functionality entirely.

Q. I'm --

A. I agree with that prohibition.
Q. I just want to make sure I'm clear because you're here opining that Georgia is taking an unacceptable level of risk with its Poll Pads as well as part of the structure of the election system. Am I correct about that?
A. Yes.
Q. And so what is the determination? Is it the fact that there's a card moving from the Poll Pad to the BMD that makes it an unacceptable level of risk and that distinguishes California and Pennsylvania, or is there something else on which you're basing your analysis that this degree of risk in using the Poll Pads is unacceptable?
A. So I'm basing that -- I'm basing that opinion on the overall vulnerability of the Poll Pads and that additional link between the Poll Pads and the BMDs, and those are the primary -- that's the primary basis for that assessment.
Q. Okay. And sitting here today, you can't say whether or not California and Pennsylvania's use of the Poll Pads is an acceptable or unacceptable level of risk; is that correct?
A. That's right. I can't say that. I haven't fully evaluated that.

Q. Let's move next to supply chain threats. You don't have any evidence in paragraph 50 that attackers have infiltrated the software development process of Dominion KnowInk, PCC, or their suppliers, right?
A. No. I'm talking about the risk that that could happen.
Q. Right. But you don't have any evidence it has happened?
A. I don't. And I'm not sure that there would be such evidence available if it had happened successfully.
Q. And then in paragraph 51, you talk about the design of several components overseas. Is it your testimony that Serbian programmers, that automatically means that this is going to be accessed by the Russians or influenced by the Russians in some way?
A. No. Not that it will automatically be, just that the risk is even higher than if the software were developed domestically in a facility that was not in a location of a government closely aligned with Russia.
Q. And the EMS runs an antivirus software made by a Czech company, you say, which earlier we said was the Avast Antivirus file shield system; is that right?
A. Avast, like a pirate.
Q. And is Avast a widely-used antivirus software?

A. It is.
Q. Why mention that it's a Czech company in that scenario? Does that increase the risk if it's a widely-used piece of software?
A. It creates further risks because the -- although a widely-used piece of software -- although it is a widely used piece of software, it's still true that if attackers were to infiltrate that company, they could spread -- spread malicious functionality into the election management system.
Q. And so it's your testimony that the antivirus is both a terrible system because it doesn't track stuff and it grants this Czech company access to the server?
A. It can be simultaneously true that it introduces new risks and doesn't adequately mitigate other risks.
Q. And your reliance for this section of your report is from this Computer World article, right?
A. I'm sorry.
Q. I'm sorry. Let me rephrase that. In paragraph 51 the statement about Dominion using Serbian programmers is based on this Computer World article, correct?
A. Yes. Although, I'm aware that that has been reported elsewhere. I'm not sure where.
Q. And this is a system that has been certified by the

EAC since 2016, right?
A. Yes. Although, again, the EAC certification process is not a -- it has significant limitations to its security review. It's not a rigorous security review.
Q. And your statement that a hostile government might attempt to plant an agent at any of these companies, black male honest employees, or hack into the software development environments, that's true of every election system and even ballot printing services, right?
A. I think it's an increased risk in foreign jurisdictions, especially jurisdictions that are aligned with potentially hostile governments.
Q. So it's a true statement. But you think that Georgia's selection of Dominion led to an increased risk of the -- of that sentence happening; is that a fair statement?
A. Yes.
Q. And how are you evaluating the increased risk by using foreign contractors versus domestic contractors?
A. This is -- well, it's just -- it's well known that -- it's well known among the -- among the -- in the -- it's well known in the study of supply chain risk

that extra jurisdictional supply chains create additional risks that are not -- that are more greater in kind than the risks of domestically produced and domestically sourced equipment.

Q. So there's not a kind of scientific evaluation of that. It's just it is what it is, right?

A. It's not quantified. It's very difficult to quantify.

Q. Got it. Paragraph 52, you say that the measures being taken to safeguard are not sufficient, and then you go through kind of some of these examples. First of all, the AuditMark process. Have you ever done research about how the AuditMark process works specifically in Dominion software?

A. I've reviewed Dominion's technical documentation about it.

Q. And in paragraph 54 you indicate that you have designed malware that runs on an optical scanner that can manipulate digital ballot images. And that's true of a hand-marked system or a ballot marking device system, right?

A. That's right.

Q. And that was not in the Dominion system. That was on a different manufacturer; is that right?

A. It works against Dominion-style ballots, among

others.
Q. Have you tested it on Dominion's ICP and ICC scanners?
A. No. But based on the way that the malware works, I have no reason to doubt that it would function on those scanners.
Q. Would it take physical access to install the malware on the scanners?
A. No.
Q. In paragraph 56 you indicate that the tampering wouldn't be detected by the election software. And I'm assuming since that's not unique to BMDs. This is another reason why you urge audits because it would be found in an audit, correct?
A. It would be found in an audit that reviewed the physical paper ballots as opposed to the digital ballots, ballot images.
Q. Do you know which method Georgia is going to use, paper or digital images?
A. So, again, this is talking specifically about AuditMark itself as a mitigation, like the AuditMark mitigation is insufficient -- sufficiently robust audits, and I do believe that Georgia intends to do its audits by going back to physical paper ballots, could detect an attack like this. The question is

whether those audits are going to be sufficiently robust.

Q. And then the next section discusses hash comparisons, and you say that Georgia may employ a method of hash comparisons. Do you know for sure whether or not it will or not?

A. I don't know for sure whether it will or not.

Q. And hashing a value of a software versus a known good hash value is used in a lot of computer security contexts, correct?

A. Yes.

Q. And at the end of paragraph 60 you say that a sophisticated attacker could conceal the presence of malware even if officials practiced hash comparisons according to Dominion's instructions. Would a better hash compare process be a more secure process?

A. Potentially, yes.

Q. Okay.

A. Can we take a break sometime soon?

Q. Sure. Yeah. We can go ahead and take a break now, if you'd like to.

A. Okay.

(Recess taken.)

BY MR. TYSON:

Q. All right. Dr. Halderman, you mention in paragraph

61 -- I think we've already covered antivirus software and end-point protection software provides only a limited defense. So it's your testimony no matter what antivirus or end-point protection a BMD or a precinct scanner had on it, that's not going to protect them against a sophisticated nation state attack, right?

A. Yes.

Q. In paragraph 62 you talk about one safeguard used in Georgia is tamper-evident seals. Are you aware of those used on the new ballot marking devices?

A. No, I'm not. But I'm aware of fairly extensive research on many different tamper-evident seals used in different kinds of election systems, and none of them offer strong security.

Q. And so for physical security, your testimony is that a tamper-evident seal is not going to provide any real physical security; is that fair to say?

A. No. Not against a remotely capable adversary.

Q. Would it provide some security against a locally working adversary?

A. Maybe against an adversary who didn't Google for how to break the seals.

Q. And so is there any value then to using seals on voting equipment?

A. I don't say that there is no value to using seals, but they don't protect against the kinds of attackers that are at issue in -- in my report, which are ones who are sophisticated hostile adversaries.
Q. So there may be good reasons to use seals for just kind of administration or documenting purposes, but not to rely on those seals for purposes of protecting against sophisticated attacks; is that a fair statement?
A. Yes.
Q. And you have not reviewed the rules generally on physical security or on the use of seals in Georgia going forward, right?
A. I have not seen those rules.
Q. Okay.
A. But this is generally true of seals used in voting.
Q. Uh-huh. And in considering other elements of physical security, you didn't consider other elements of physical security for Georgia ballot marking devices, only seals in reaching your conclusions for this report, right?
A. I've considered what I've known about Georgia physical security procedures in the past. But if they have been changed, then I'm unaware of what other protections are in place.

Q. Next we call logic and accuracy testing. Are you aware what the logic and accuracy protocols are for Georgia's new ballot marking devices?
A. I'm not, but it doesn't matter. No logic and accuracy testing protocol is going to provide strong protection against the kinds of attacks that I'm discussing.
Q. And you're not aware of any research that shows how a piece of software could distinguish between a test voter and an actual voter based on, for example, the rate at which people vote; is that correct?
A. It's certainly possible, and I've written malware that attempts to do that. And, in fact, our ballot marking device study published in January discusses some ways that malware could use different features to try to distinguish between different categories of voters, which I think touches on the subject of test votes versus non.
Q. And for parallel testing in paragraph 65, are you aware of what Georgia's protocols are going to be for parallel testing with the new ballot marking devices?
A. I don't believe Georgia has made those public. I'm not aware. But in general, it's impossible for parallel testing to definitively or even reliably detect misbehavior by a ballot marking device.

Q. And that's true even if at a random point in the middle of the day every county went to every ballot marking device and generated a certain number of ballots?
A. Yes. Unfortunately it is true in that case. And the mathematical derivation is in the paper I cite.
Q. You say at the end of paragraph 67, to your knowledge, the state does not maintain sufficient quantities of pre-printed ballots to allow voting to continue under such a circumstance when the BMDs fail. Have you reviewed the state election board rules regarding back-up ballots and what's required?
A. I haven't reviewed them, but that's my understanding from evidence that's come to light in the Curling case about Georgia's current plans.
Q. And do those include the changes that were made last month to Georgia's rules regarding the number of paper ballots?
A. I don't know. I don't know the timing.
Q. So it's possible then that the state is now going to require counties to maintain sufficient quantities to allow voting to continue if the BMDs go out, and you just don't know if that's the case, right?
A. My understanding is that the -- the state plans to have a very limited number of ballots available and

to print more on demand, if necessary. But the problem is if all of the BMDs across a large region were to be sabotaged, as is possible by a malicious software spreading from say a county election management system, then you'd have a simultaneous failure and require a very large number of ballots sufficient for all voters, which would be impossible to produce on -- and distribute in time.

Q. You say in the post-election audit portion that officials could potentially detect certain kinds of attacks by a rigorous audit of paper ballots. Actually, before I get to that, that footnote at the bottom of page 28, the Philip Stark paper.

A. Yes.

Q. Is that a peer-reviewed paper?

A. I don't know whether he's had the paper since peer-reviewed. I have independently -- I have assessed myself the correctness of the -- of Stark's result, but I don't know if it's gone through formal peer review or not.

Q. So next we have sufficient audits. And I think we've talked through the various categories of how audits can detect things already. The good thing is we've covered a lot of this, so I can move through here.

All right. So let's skip ahead to

paragraph 72. You say that the ballot marking devices are computers, run outdated and vulnerable software, must be programmed using the election management system before every election. This is -- kind of unlike DREs, this is an election system, recommended by the National Academy of Sciences. I know that DREs were certified by the EAC -- certified by the US Election Assistance Commission. Why are you taking the position that these are -- should never be used by all voters in an election?

A. Right. So I'm taking that position based on subsequent research that was called for by the national academies in their study that has -- that has established that the rate at which voters review and catch errors in BMD-printed ballots is very low and is, in fact, likely to be so low that an attack on the BMDs in a close election wouldn't be detected by election officials.

Q. And so the subsequent research you're relying on are the two studies about the rate of voter verification of BMD ballots, right?

A. That's right. Although, there is previous work on VVPATs systems that was highly suggestive that there might well be a problem with BMDs. So these new results confirm and extend the problems with VVPATs

to BMD-based systems.
Q. And those prior studies with VVPATs were prior to the National Academy of Science's recommendation, right?
A. That's right. But there was still at least some substantial question about whether the findings would apply with equal certainty or equal force to BMD systems, but now there's now strong evidence that the same problems occur.
Q. All right. So let's get to those two studies. If you want to jump ahead with me to paragraph 81. So the first study that you cite about the rate at which voters verify or look at their ballot marking device printed ballots was a study by Dr. DeMillo, Robert Kadel, and Marilyn Marks; is that right?
A. That's correct.
Q. And you'd agree with me that Ms. Marks is an activist for hand-marked paper ballots; is that a fair assessment of her?
A. Well, I'd agree that she's an election integrity activist.
Q. And she opposes electronic voting as a policy matter, right?
A. I'm not sure she opposes all electronic voting, but she opposes paperless electronic voting.
Q. Does she -- do you know, she opposes ballot marking

devices for all people?
A. I believe she does, yes.
Q. And this study has not been peer-reviewed, has it?
A. No, that study has not.
Q. And when voters in the study spent only four seconds reviewing their ballots, how many races were they looking at, do you know?
A. I don't know. I don't know off the top of my head.
Q. And do you know if that study evaluated the use of signs or verbal cues or other things to ask voters to verify their ballots?
A. No. That we evaluate -- that my research group evaluated in the other study I cite.
Q. So let's go to that one. Paragraph 82 you have a realistic simulated election. Were the candidate names in the election something that individuals would recognize?
A. Yes.
Q. And what were the candidate names?
A. The candidate names were the names of the candidates from the most recent Michigan midterm.
Q. Let me hand you what we've marked as 15.
(Exhibit No. 15 marked.)
BY MR. TYSON:
Q. And is this your study with Mr. Bernard?

A. Yes. And five other authors.
Q. And Mr. Bernard is a student of yours, correct?
A. Yes. He's a Ph.D. student.
Q. And have you found him to be reliable and a good student?
A. Yes.
Q. Now, in the various scenarios that are outlined here, you found that verbal prompting increased the number of voters who were reviewing their ballots, correct?
A. I did.
Q. And you found that verbal prompting accompanied by kind of identification of candidates on a slate significantly increased the number of voters who reviewed their ballots, right?
A. Yes, it did.
Q. And so in terms of a policy recommendation going forward, is it your position that there is no way a state can increase the number of voters verifying their ballot marked device ballots based on your research?
A. The question is whether the increase is likely to be significant enough that the state will have a high chance of detecting attacks against a close election. And the problem is that the magnitude of increase that we found even with the best verbal prompts was

relatively small. And the magnitude, though, larger that we found with the use of slates only applies to the subset of voters who actually use slates. So unless use of slates can be the vast majority of voters, even under the best of conditions, that mitigation would not result in a high probability of detecting attacks on close elections.

Q. And this is the first peer-reviewed study of its kind, studying this specific question of voter verification and ballot marking devices, right?

A. Yes. Though I understand there are others now under review that will be published soon.

Q. And are you aware whether Georgia requires poll workers to give verbal prompts to voters?

A. I know that Georgia law requires signs, which we find are not effective. There may -- I don't know if there are recently issued rules that also require a verbal prompt.

Q. So if the state election board issued rules requiring a verbal prompt, that would at least move up the chain a little bit in terms of verification, right?

A. It would likely move it up. But again, the rate that -- the rate that would be required in order to cause a significant -- excuse me. In order to have a high likelihood of detecting fraud even in close

elections is something like ten times the improvement that we measured in the study from verbal prompts alone. So there's a lot more work that would need to be done or a lot more increase that would be needed in addition to verbal prompts.

Q. But ultimately it's fair to say that the study found that a well-designed procedure can have a significant impact on the rates of voters checking their ballots, right?

A. Significant in the sense of statistically significant or reliably measurable, but not necessarily in terms of adequate.

Q. And the paper also concludes that more research is needed in this area. Do you agree with that, right?

A. I do.

Q. And you welcome additional research on this topic?

A. I do.

Q. And if you -- if that later research demonstrates that voters check their ballots at a high enough rate, as you've outlined in this paper from a mathematical perspective, would that change your view of the use of ballot marking devices?

A. Yes.

Q. You opine in paragraph 87 that election officials are unlikely to take disruptive actions unless there's a

certain or a fraction of BMD voters that are reporting problems. What are you basing the fact that election officials are unlikely to take disruptive actions on?

A. In part the fact that there are a certain number of reports of problems and inconsistencies in every election. And so election officials don't as a general rule say we're going to have to take all of our machines aside and study them just because there was some sporadic reports of problems that could be explained away by other things. The rate would have to be elevated in a way that stood out and was unmistakable in order to take drastic action.

Q. And your issue focused particularly on the margin of victory being relevant to this consideration, right? The analysis, the mathematical analysis.

A. I'm sorry.

Q. Let me rephrase that question. In determining the mathematical analysis you outline in this report, the margin of victory was significant, right?

A. Yes.

Q. And so in a larger margin of victory, would that mean fewer voters would have to report a problem? Where does the scale go in terms of larger margin of victory versus smaller margin of victory?

A. I see. If the margin of victory is smaller, then it's easier to attack the system, if that's the -- the question you're asking.
Q. Yeah. Thank you.
A. It takes us back to the election official's prayer, please let it not be close.
Q. That's right. And the election lawyer's prayer usually as well.
A. And the election security researcher's prayer.
Q. Okay. Paragraph 88. Now we get to the question of the DREs.
A. I'm sorry. Paragraph --
Q. We can put aside the exhibit. Yeah. Exhibit 15 is finished. So paragraph 88 of your report.
A. Okay.
Q. We move to the DRE machines, correct?
A. Yes. Okay.
Q. And you're aware DREs are never going to be used in Georgia again, right?
A. Yes. Thank goodness.
Q. And those were decertified by the Secretary of State at the end of 2019?
A. That's right, as my research suggested in 2006.
Q. And you state at the bottom of 88 that the DRE system was highly susceptible to cyber attacks. But as

we've discussed, there's no evidence that any of the DREs in Georgia were ever actually compromised, right?

A. That's right. But again, I don't think anyone has ever actually inspected the software running in any of those DREs.

Q. And you cite the broad scientific consensus about DREs not providing adequate security and you cite to the Securing the Vote from the National Academy of Science's report, right?

A. Yes.

Q. But you don't rely on that report for its recommendations about ballot marking devices because of the subsequent reports we've discussed, right?

A. That's right. The science about ballot marking devices has moved. There has not been any movement in the scientific consensus of -- regarding DREs.

Q. And the virus that you reference and discuss kind of from 90 to 93, you've never tested that virus on the version of software used in Georgia on the DREs, right?

A. No. But actually, that's a good question. It would be -- so I have tested viral software on the previous version and the subsequent version of the firmware used in the DREs but not on the firmware version used

in Georgia because that was not available to me until recently.

Q. But it is available to you now?

A. In the Curling matter.

Q. And you have not yet made any analysis of that at this point?

A. It didn't occur to me until you asked the question that that would be possible to do.

Q. And how did you obtain access to that version of the software in the Curling matter?

A. It is in the -- it's contained in the FBI image from Kennesaw State University Center For Election Systems. At least I believe that's correct. I -- I may be mistaken about that, but I do believe that the firmware is there. If my recollection is correct --

Q. Got it.

A. -- that analysis is not complete.

Q. In paragraph 95 you reference the GEMS and vulnerabilities in GEMS and BallotStation. And I know we talked about the election management servers before. But you've looked at the GEMS databases for Georgia and have not found any infiltration or any sort of manipulation of those databases, right?

A. Yes. The data -- the databases themselves is distinct from the full contents of the server

computers, which are -- which would be the -- the more complete way to -- a more reliable way to look for an infiltration.

Q. And in 99 you say, in your opinion, an attacker who infiltrated the SOS GEMS system could have spread malware to the county GEMS servers be infecting the CDs used to distribute the files. And you have not in your review of those CDs or any of the GEMS databases found where that has occurred, right?

A. I haven't had -- I don't have access to the CDs that were distributed, only to the GEMS databases. So I can't assess whether the CDs actually did contain malware, just that that is a viable threat factor.

Q. And at the end of paragraph 100 when you say that Georgia's election security countermeasures were inadequate to doing these various things, the last one is altering election outcomes. It's not your testimony that Georgia election outcomes have been altered, is it?

A. It's my testimony that we don't know and that the election system did not generate adequate evidence, at least any evidence that has been reviewed to date to conclude that past election results were, in fact, accurate.

Q. Is it your testimony that we should doubt the results

of the November 2018 election in Georgia?
A. I wouldn't go that far. I don't want to -- I don't want to go that far. But I do think that there is -- I think all of the ingredients were there for an attacker to access the voting machines in polling places and change the results. The question is did anyone actually do that or not. And we wouldn't be able to tell the difference from the evidence that is outwardly visible one way or the other. That's an unfortunate consequence of the way the election system was designed and operated.
Q. So then why not doubt the November 2018 election results.
A. Because the election has been decided and history has moved on.
Q. So in your opinion, there's no value to go back and try to do forensic analyses and dig up whether we should rely on those results or not?
A. Actually, I think that is very valuable because that will teach us more about how Georgia needs to secure the 2020 election.
Q. How would it help with that question if it's analyzing a system that's never going to be used again?
A. Because not all components of the system are being

replaced.
Q. Which components of the system are not being replaced?
A. The eNet system, the general network infrastructure and computing infrastructure at the Secretary of State, other infrastructure at the county level that is used by election administrators.
Q. So if history needs to move on and the election has been decided, why not just do forensic analyses of eNet, the network infrastructure of the Secretary of State, the network infrastructure of county offices?
A. That's going to be a less reliable way and much more complicated way of trying to answer some of the similar questions.
Q. And you referenced the design of Georgia's election system. You're not testifying that anyone intentionally designed a system that would be vulnerable to hacking, are you?
A. Intentionally designed, no. Negligently maintained? In my opinion, yes.
MR. TYSON: Off the record for just a minute.
(Recess taken.)
MR. TYSON: All right. Back on.

BY MR. TYSON:

Q. Dr. Halderman, thank you for your time today. I don't have any further questions.

A. Thank you.

MR. HERMAN: All right.

(Deposition concluded at 3:37 p.m.)

* * *

CERTIFICATE OF NOTARY PUBLIC

STATE OF MICHIGAN )
)
COUNTY OF LENAWEE )

I, Trisha Cameron, Certified Shorthand Reporter and Notary Public in and for the State of Michigan, do hereby certify that the witness whose attached deposition was taken before me in the above cause was first duly sworn or affirmed to testify to the truth, the whole truth, and nothing but the truth; that the testimony contained herein was by me reduced to writing in the presence of the witness by means of Stenography; afterwards transcribed by means of computer-aided transcription; and that the deposition is a true and complete transcript of the testimony given by the witness to the best of my ability. I further certify I am not connected by blood or marriage with any of the parties, their attorneys or agents; that I am not an employee of either of them; and that I am not interested directly, indirectly, or financially in the matter of controversy.

Trisha Cameron, RDR, RMR, CRR, RPR, CSR
Notary Public, Lenawee County, Michigan
My Commission Expires 5-24-24

**c**

**d**

Georgia Code

Title 9, Chapter 11

Article 5, Section 9-11-30

(e) Review by witness; changes; signing.
If requested by the deponent or a party before completion of the deposition, the deponent shall have 30 days after being notified by the officer that the transcript or recording is available in which to review the transcript or recording and, if there are changes in form or substance, to sign a statement reciting such changes and the reasons given by the deponent for making them. The officer shall indicate in the certificate prescribed by paragraph (1) of subsection (f) of this Code section whether any review was requested and, if so, shall append any changes made by the deponent during the period allowed. If the deposition is not reviewed and signed by the witness within 30 days of its submission to him or her, the officer shall sign it and state on the record that the deposition was not reviewed and signed by the deponent within 30 days. The deposition may then be used as fully as though signed unless, on a motion to suppress under paragraph (4) of subsection (d) of Code

Section 9-11-32, the court holds that the reasons given for the refusal to sign require rejection of the deposition in whole or in part.

DISCLAIMER: THE FOREGOING CIVIL PROCEDURE RULES ARE PROVIDED FOR INFORMATIONAL PURPOSES ONLY. THE ABOVE RULES ARE CURRENT AS OF APRIL 1, 2019. PLEASE REFER TO THE APPLICABLE STATE RULES OF CIVIL PROCEDURE FOR UP-TO-DATE INFORMATION.

VERITEXT LEGAL SOLUTIONS
COMPANY CERTIFICATE AND DISCLOSURE STATEMENT

Veritext Legal Solutions represents that the foregoing transcript is a true, correct and complete transcript of the colloquies, questions and answers as submitted by the court reporter. Veritext Legal Solutions further represents that the attached exhibits, if any, are true, correct and complete documents as submitted by the court reporter and/or attorneys in relation to this deposition and that the documents were processed in accordance with our litigation support and production standards.

Veritext Legal Solutions is committed to maintaining the confidentiality of client and witness information, in accordance with the regulations promulgated under the Health Insurance Portability and Accountability Act (HIPAA), as amended with respect to protected health information and the Gramm-Leach-Bliley Act, as amended, with respect to Personally Identifiable Information (PII). Physical transcripts and exhibits are managed under strict facility and personnel access controls. Electronic files of documents are stored in encrypted form and are transmitted in an encrypted fashion to authenticated parties who are permitted to access the material. Our data is hosted in a Tier 4 SSAE 16 certified facility.

Veritext Legal Solutions complies with all federal and State regulations with respect to the provision of court reporting services, and maintains its neutrality and independence regardless of relationship or the financial outcome of any litigation. Veritext requires adherence to the foregoing professional and ethical standards from all of its subcontractors in their independent contractor agreements.

Inquiries about Veritext Legal Solutions' confidentiality and security policies and practices should be directed to Veritext's Client Services Associates indicated on the cover of this document or at www.veritext.com.